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

ANALYSES

JURISPRUDENCE : SPECIAL POURRIEL

TEXTES OFFICIELS

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 adminstratives indépendantes et des textes normatifs.

Conseil scientifique

Informations légales

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

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

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

Directeur de publication , directeur scientifique, PAO : Julien Le Clainche

DROIT-TIC .com

R.D.T.I.C

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

ANALYSES

JURISPRUDENCES

TEXTES OFFICIELS

DROIT-TIC .com

R.D.T.I.C

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

ADRESSAGE, NOMS DE DOMAINE ET LIENS HYPERTEXTES

CONDAMNATION D'UN REGISTRAR AUX FRAIS DE JUSTICE

M. Cédric Manara, Professeur associé, EDHEC Business School et

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

La 14ème chambre du Tribunal correctionnel de Lyon, dans un jugement du 21 juillet 2005 vient préciser le régime juridique des organisateurs de forum de discussion.

Le régime juridique des organisateurs de forum discussion

Tribunal correctionnel de Lyon, 14ème chambre, 21 juillet 2005 :

La 14ème chambre du Tribunal correctionnel de Lyon, dans un jugement du 21 juillet 2005 vient préciser le régime juridique des organisateurs de forum de discussion.

En l'espèce, le Groupe Mace alléguait qu'en publiant par écrit sur le forum de discussion du site www.acheteenligne.com des messages dissuadant les lecteurs d'acheter chez « Point Mariage » ou chez « Complicité » leurs tenues de mariage et en dénigrant ces deux enseignes, Gilbert D., exploitant dudit site web, avait porté atteinte à l'honneur ou à la considération du Groupe Mace, en application des dispositions de la loi du 29 juillet 1881.

Le demandeur, après avoir fait constaté par voie d'huissier les propos diffamatoires tenus à son encontre, a mis en demeure Gilbert D. de supprimer les contenus litigieux. Ce dernier s'est exécuté.

Le Groupe Mace, constitué partie civile, a ensuite assigné Gilbert D. en diffamation publique envers un particulier devant le Tribunal correctionnel de Lyon.

À l'appui de ses prétentions, la partie civile invoque l'article 93-3 de la loi du 29 juillet 1982 sur la communication audiovisuelle pour obtenir la condamnation de Gilbert D., en sa qualité de directeur de la publication du site en cause.

Le Tribunal précise que la responsabilité éditoriale, telle que prévue dans la loi de 1982, suppose la fixation préalable du contenu litigieux.

Il rejette dès lors l'application de la loi de 1982 aux organisateurs de forum de discussion modéré a posteriori,« *un organisateur de forum ne dispos[ant] pas de la capacité de prendre connaissance des messages avant la communication au public* ».

Le Tribunal se base ainsi sur la recommandation du forum des droits sur l'Internet du 8 juillet 2003 et sur les travaux parlementaires de la loi du 21 juin 2004 pour décider que « *le responsable d'un forum non modéré ou modéré a posteriori doit être considéré comme un hébergeur au sens de la loi puisqu'il assure le stockage direct des messages diffusés sans porter de regard préalable sur ces derniers* ». Ce faisant le Tribunal calque le statut du responsable du forum de discussion sur celui du prestataire d'hébergement défini à l'article 14 de la directive européenne du 8 juin 2000.

Les juges font donc application, en l'espèce, « *du régime de responsabilité "allégée" prévu par la loi du 21 juin 2004* »qui exonère de responsabilité le prestataire qui agit promptement pour supprimer tout contenu illicite dès qu'il en a eu connaissance.

Ayant constaté que Gilbert D. avait éliminé le message considéré comme diffamatoire dans les 24 heures de la demande formulée par le Groupe Mace, le Tribunal a débouté la partie civile de sa demande en réparation du préjudice.

Par M. Cédric Manara, Professeur associé, EDHEC Business School et M. Jean-François Poussard Rédacteur en Chef MailClub.info

DOMAIN NAME / NOM DE DOMAINE !

DECEMBER 21, 2005

.cat is live

ICANNWatch reports.

DECEMBER 20, 2005

ICANN seeks an in-house counsel for contract law matters

Of possible interest for readers of this blog. The job is based in Brussels. Announcement here.

DECEMBER 19, 2005

"Staggernation"

This website has collected so many bad faith defense arguments in WIPO disputes that it is unable to decide what is the most dubious! Examples (no comment...):

Respondent asserts that his fiancée was Chanel Louise Wright, and they together at one time also had an e-commerce business...
Respondent states that he and his girlfriend/fiancée Chanel "narrowed it (the choice of original title of our business) down to the following three choices:
*a) **chanelbags.com***
*b) **chanelpurses.com***
*c) **wholesalepurses.com***
"Chanel and I used wholesalepurses.com because of the fact that Chanel and I broke off our wedding engagement

LEGAL

Disclaimer

Déclaration CNIL n° 1037258

A PROPOS DE CE BLOG

Blog choisi par Le guide des blogs Francophones 2006

PREVIOUS POSTS

.cat is live
ICANN seeks an in-house counsel for contract law matters
"Staggernation"
eBay / Perfume Bay
Ed Hasbrouck calls for an independant review of IC...
Domain name news
ADR.Center for .eu disputes launches its official website
Lancement du site de la Czech Arbitration Court
Echo

http://domaine.blogspot.com/

http://www.mailclub.info

DROIT-TIC .com

R.D.T.I.C

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

PROPRIÉTÉS INTELLECTUELLES, PROPRIÉTÉS INDUSTRIELLES ET COMMERCIALES

UNE NOUVELLE INTERPRÉTATION DES ARTICLES L.714-5 DU CPI ET 5 C-2 DE LA CUP

Par Me. Nicole Bondois, Avocate et Melle Amélie CAPON Juriste en propriété industrielle

La chambre commerciale de la Cour de cassation vient d'opérer un revirement de jurisprudence quant à l'interprétation de l'alinéa 2b) de l'article L.714-5 du CPI, dans trois arrêts du 14 mars 2006.

La chambre commerciale de la Cour de cassation vient d'opérer un revirement de jurisprudence quant à l'interprétation de l'alinéa 2b) de l'article L.714-5 du CPI, dans trois arrêts du 14 mars 2006.

En 1992, la Cour de cassation avait, dans une décision remarquée[2], jugé qu'en déposant deux marques qui ne différaient que très légèrement l'une de l'autre, son titulaire manifestait ainsi sa volonté d'obtenir des droits privatifs distincts sur ses deux marques qu'il n'estimait pas assimilables l'une à l'autre.

Il en résultait que l'exploitation de l'une ne permettait pas d'éviter la déchéance de l'autre.

La haute Cour se fondait sur les articles 5 C-2 de la CUP[1] et L.714-5 du CPI, considérant que ces textes ne trouvaient, toutefois, application que si une seule marque était en cause.

Elle opérait donc une distinction selon que la marque seconde exploitée au lieu de la première en date était ou non enregistrée.

Si la marque seconde était enregistrée, les juges considéraient qu'elle constituait une marque distincte de la première, de sorte que l'usage de l'une ne valait pas exploitation de l'autre au sens de l'article L.714-5 du CPI.

Il en allait autrement lorsque la marque seconde n'était pas déposée.

Les tribunaux admettaient, dans ce cas, que l'utilisation d'un signe légèrement modifié valait usage du signe enregistré antérieurement à condition, toutefois, que ses éléments distinctifs n'aient pas été altérés.

Ce courant jurisprudentiel s'est maintenu en dépit d'un arrêt de la Cour d'appel de Paris en date du 21 janvier 2000[3], venu, il est vrai, quelque peu ébranler les certitudes en la matière.

Les juges du second degré avaient estimé, en effet, que « *la déchéance étant une sanction, les conditions de son application [devaient] être interprétées restrictivement* ». Ils ajoutaient que les articles 5 C-2 de la CUP et L.714-5 du CPI « *faisant référence à l'emploi sous une forme modifiée sans distinguer si cette forme modifiée fais[ait] ou non l'objet d'un enregistrement distinct à titre de marque, il en résult[ait] que le titulaire de deux marques qui n'exploite que la seconde en date doit pouvoir échapper à la déchéance de ses droits sur son premier dépôt si les différences entre l'une et l'autre sont minimes et n'altèrent pas le caractère distinctif essentiel du premier signe* ».

Dès lors et en l'espèce, il avait été décidé que l'exploitation de la marque « Poême » faisait échapper à la déchéance, la marque « Poeme ».

Mais s'agissant d'un arrêt de Cour d'appel, il n'a eu, en pratique, que peu de retentissement et n'a pas permis de

mettre fin à la jurisprudence élaborée en 1992 par l'Assemblée plénière.

Récemment encore, le Tribunal de grande instance de Paris, dans un jugement du 1er décembre 2005[4] devait décider que l'utilisation du signe « *Ame de Parfum* » valait exploitation de la marque déposée en lettres bâton avec un accent circonflexe ÂME DE PARFUM, considérant d'une part, que l'accent circonflexe ne constituait qu'un des éléments distinctifs de la marque, d'autre part, que sa suppression ne modifiait pas la signification de l'expression dont la prononciation restait inchangée.

C'est en fait la signification de la locution « *Ame de parfum* » qui confère à la marque son caractère distinctif principal.

La Cour d'appel de Paris, dans un arrêt du 20 janvier 2006[5], a quant à elle considéré, que l'exploitation de la marque SPA ne permet pas d'échapper à la déchéance de la marque SPA THERMES. Elle ajoute qu'en déposant ces deux marques, le titulaire a reconnu implicitement qu'elles présentent des pouvoirs distinctifs différents.

Cette jurisprudence a pour objet de faire échec au dépôt de marques de défense, c'est-à-dire de marques se rapprochant sensiblement d'une marque première afin d'empêcher un éventuel concurrent de s'approprier indûment le signe distinctif d'un autre, ce qui est contraire au principe de la liberté du commerce et de l'industrie.

Notons à cet égard, qu'à côté de l'article L.714-5 du CPI, le titulaire légitime de marques dispose d'un arsenal de dispositions comme le principe de spécialité, la contrefaçon par imitation ou la concurrence déloyale lui permettant de protéger son signe tout en respectant la règle de libre concurrence.

Cette interprétation de l'alinéa 2b) de l'article L.714-5 du CPI a prévalu jusqu'au 14 mars 2006, date à laquelle la chambre commerciale de la Cour de cassation a revu sa position dans trois arrêts[6] rendus dans des espèces rigoureusement similaires.

Les défendeurs, poursuivis en contrefaçon de marques, avaient demandé reconventionnellement la déchéance pour défaut d'exploitation des marques qui leur étaient opposées.

A l'appui de leur argumentation, ils ont fait valoir que l'exploitation d'une marque enregistrée, analogue à une autre marque enregistrée ne vaut pas exploitation de cette dernière au sens de l'article L.714-5 du CPI, et ce conformément à la solution dégagée par l'Assemblée plénière de la Cour de cassation.

La chambre commerciale vient sanctionner cette argumentation en reprenant dans des termes quasiment identiques le même attendu : les articles 5 C-2 de la CUP et L.714-5 du CPI « *exigent seulement que la marque exploitée ne diffère de la marque enregistrée et non exploitée que par des éléments n'en altérant pas le caractère distinctif, peu important que la marque modifiée ait été elle-même enregistrée* ».

La Cour de cassation revient ici à une application plus stricte de ces textes. Elle estime ainsi que l'ancienne jurisprudence ajoutait une condition aux articles précités, à savoir que la marque modifiée ne devait pas avoir été enregistrée pour faire échec à la déchéance de la marque première.

La haute Cour prend, selon nous, clairement parti en faveur des titulaires de marques sans pour autant légitimer la pratique des marques de barrage.

Rappelons à cet effet que l'exploitation de la marque sous une forme modifiée n'est prise en compte que si cette modification n'en altère pas le caractère distinctif.

La jurisprudence rendue sur ce point reste d'actualité.

Les juridictions devront dès lors être vigilantes et sanctionner tout comportement abusif de la part de titulaires de marques qui seraient tentés de déposer de multiples déclinaisons de leur signe à seule fin d'étendre leur monopole d'exploitation et échapper ainsi à une déchéance de leurs droits.

Par Me. Nicole Bondois, Avocate et Melle Amélie CAPON Juriste en propriété industrielle

1 Convention d'Union de Paris du 20 mars 1883, ci-après désignée CUP.

2 Ass. plén. Ccass., 16 juillet 1992, PIBD 1992, III, 659.

3 CA Paris, 4ème Ch., 21 janvier 2000, SNC Lancôme Parfums et Beauté c/ SARL Papous, PIBD 2000, n°697, III, 234.

4 TGI Paris, 3ème ch., 2ème sect., 1er décembre 2005, Frederic'M France SA c/ Guerlain SA, PIBD 2006, n°825, III, 182.

5 CA Paris, 4ème B, 20 janvier 2006, L'Oréal SA et Helena Rubinstein SNC c/ SPA Monopole Compagnie Fermière de Spa SA, PIBD 2006, n°826, III, 217.

6 Cass.com, 14 mars 2006, arrêt n°369, M.Franklin c/ Sté Pier Import Europe ; arrêt n°370, Playboy entreprises international inc. c/ Sté Etablissement Laporte ; arrêt n° 371, Sté Trader Media c/ sté Centrale directe SARL, www.courdecassation.fr.

DROIT-TIC .com

R.D.T.I.C

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

INFORMATIQUE ET LIBERTÉS, DROIT SOCIAL, DROIT DU TRAVAIL

CONTRÔLES BIOMÉTRIQUES : LES RÈGLES À RESPECTER EN FONCTION DES TECHNIQUES UTILISÉES

Par M. Nicolas Samarcq,
Juriste TIC

Depuis quelques années les organismes privés et publics ont recours aux techniques biométriques pour renforcer la sécurité des accès aux locaux ou contrôler les horaires de travail.

Les systèmes biométriques s'appuient en particulier sur la reconnaissance de l'empreinte digitale, du contour de la main ou de l'iris

Face au risque de réutilisation de ces données personnelles, notamment les empreintes digitales qui laissent des « traces » et permettent une identification *a posteriori* des personnes présente dans un lieu à un moment déterminé, la Commission Nationale Informatique et Libertés a publié des recommandations à l'intention des responsables de traitement.

Les positions arrêtées par la CNIL conditionnent la mise en œuvre des *« traitements automatisés comportant des données biométriques nécessaires au contrôle de l'identité des personnes*[1]», qui font l'objet d'une demande d'autorisation préalable auprès de l'autorité administrative indépendante.

Empreintes digitales

La CNIL considère que les données biométriques d'une personne, qui laissent des « traces », doivent être uniquement conservées sur un support individuel (carte à puce, ordinateur...), afin d'éviter toute utilisation étrangère à la finalité initiale du traitement. Au regard du principe de proportionnalité, elles ne doivent pas être stockées dans une base centrale ou un lecteur biométrique regroupant les caractéristiques anthropométriques de plusieurs personnes. Seules des exigences impérieuses en matière de sécurité ou d'ordre public peuvent justifier une telle centralisation des données. La CNIL précise qu'elle n'a jamais constaté l'existence d'un tel impératif de sécurité dans le cadre des activités des collectivités locales.

Sur la base de ces principes, la Commission a refusé un traitement consistant à horodater les entrées et sorties de 600 agents du centre hospitalier de Hyères grâce à un dispositif de reconnaissance des empreintes digitales, qui devait les enregistrer dans un lecteur biométrique.

En revanche, l'établissement public Aéroports de Paris a obtenu l'autorisation de mettre en place, à titre définitif, un contrôle d'accès aux zones de sûreté des aéroports d'Orly et de Roissy reposant sur la reconnaissance de l'empreinte digitale des personnes employées. En l'espèce, le gabarit de l'empreinte digitale n'est stocké que sur une carte individuelle (badge) détenue par l'employé, et les données enregistrées dans les serveurs dédiés au contrôle des accès se limitent aux données nécessaires à l'identification de la personne concernée (nom, prénom, photographie, fonction).

Contour de la main

S'agissant du contour de la main, qui ne laisse pas de « traces », la CNIL estime que la conservation de ces données biométriques peut être réalisée indifféremment sur un support individuel ou dans une base de données. La Commission autorise, par exemple, ce système pour contrôler l'accès aux cantines scolaires (6 autorisations) et refuse tout procédé d'enregistrement des empreintes digitales des élèves dans une base de données[2]

En 2005 quatre organismes ont obtenu l'autorisation de mettre en oeuvre des systèmes d'identification par le contour de la main : Carrefour, Claranet (fournisseur d'accès internet pour entreprises), le collège Les Mimosas (Mandelieu/Alpes-Maritimes) et la mairie de Gagny (Seine-Saint-Denis).
Le système biométrique de Carrefour permet de contrôler l'accès à une zone contenant des produits de valeur, celui du FAI limite l'accès du « data center » au personnel habilité. Le collège gère les entrées à la cantine pour lutter contre la fraude, et la mairie a remplacé les badges (trop souvent perdus) par le contour de la main pour la gestion du temps de travail.
En pratique, pour s'identifier, les salariés, agents et collégiens composent leur code personnel et appliquent une main sur un lecteur. Le code correspond à une « clé biométrique » (mesures de la main) associée à l'identité de la personne. Le système ne reconnaît pas l'individu à la main, il vérifie seulement que le code correspond bien à l'individu qui appose la main et aucune image ou photographie de mains n'est conservée.

* * *

Cette année le débat sur la biométrie sera relancé au niveau national avec le projet INES II, qui devrait être présenté au cours du premier semestre 2006.

Le programme INES I (Identité Nationale Electronique Sécurisée), présenté en 2005, était un projet global consistant à fusionner et sécuriser les procédures de demande de passeport européen biométrique[3] et de carte nationale d'identité électronique afin de lutter contre les fraudes à l'identité, sources de nombreuses infractions (immigration illégale, fraude aux allocations, aux droits sanitaires et sociaux, escroqueries…).

Il fut retiré en raison des nombreuses critiques et craintes prononcées au regard des atteintes à la vie privée des citoyens, notamment, dans le rapport du Forum des droits sur l'internet (16 juin 2005)[4] et la position de la CNIL (31 mai 2005)[5].

Par M. Nicolas Samarcq,
Juriste TIC

1 Article 25-I°-8 de la loi Informatique et Libertés du 6 janvier 1978, modifiée le 6 août 2004 : *« les traitements automatisés comportant des données biométriques nécessaires au contrôle de l'identité des personnes »* doivent faire l'objet d'une demande d'autorisation préalable auprès de la CNIL.

2 Lors de sa séance du 12 janvier 2006, la CNIL a validé 2 dispositifs de contrôle d'accès à une cantine scolaire reposant sur la reconnaissance du contour de la main. Elle a refusé d'autoriser 4 traitements de contrôle d'accès et de gestion des horaires reposant sur la reconnaissance des empreintes digitales (3 enregistrés dans une base de données et 1 dans un lecteur biométrique) parce qu'ils n'étaient justifiés par aucun impératif particulier de sécurité. Echos des séances, 30 janvier 2006, http://www.cnil.fr/index.php?id=1938&news[uid]=304&cHash=1b5bb06ad5.

3 Règlement européen du 13 décembre 2004.

4 http://www.foruminternet.org/activites_evenements/lire.phtml?id=111

DROIT-TIC .com

R.D.T.I.C

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

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

OUVERTURE GÉNÉRALE DU .EU ET DU .FR

Par M. Nicolas Samarcq, Juriste TIC et M. Patrick Hauss

Les citoyens européens pourront enregistrer leur nom de domaine .EU dès le 7 avril, tandis que les particuliers français devront attendre le 20 juin pour l'extension nationale .FR.

Depuis l'ouverture de la première phase d'enregistrement prioritaire « sunrise » du .EU[1], en décembre 2005, l'EURid (Registre du .EU) a reçu plus de 300 000 demandes d'enregistrement.

Près de 76 000 demandes n'ont pas abouti en raison d'erreurs techniques de registrars (bureau d'enregistrement accrédité par EURid) ou de clients n'ayant pas correctement géré leurs dossiers. De plus, 11 673 demandes ont été rejetées par PriceWaterhouseCoopers Belgique, l'agent officiel de validation des .EU.

La période « sunrise », qui se termine le 6 avril 2006, est en effet relativement complexe. Une fois la demande d'enregistrement reçue par EURid, le postulant dispose d'un maximum de 40 jours pour envoyer les documents attestant ses droits sur le nom choisi. Ceux-ci doivent être libellés et présentés selon des règles et un format très strict. Tout manquement aux règles de PwC Belgique vaut annulation pure et simple du dossier.

Les noms de domaine acceptés sont ensuite activés 40 jours après la décision de validation par PwC Belgique. Ce délai doit permettre à EURid, avant toute activation d'un nom de domaine, de s'assurer qu'une procédure de règlement de litiges alternatifs n'a pas été initiée. Elle permet donc à un titulaire de droit, qui serait arrivé second ou plus sur un domaine en .EU, de contester la décision d'attribution du domaine pendant un délai de 40 jours. Le 30 mars dernier, EURid a porté cette période à 45 jours pour la procédure dite « sunrise appeal period ».

Une semaine avant l'ouverture de l'extension .EU à tous les européens, sans justificatifs de droits à produire, EURid a annoncé avoir activé plus de 16 500 noms domaine européens. Au palmarès de la nouvelle extension européenne, la France se classe seconde avec 2 797 noms de domaine actifs, derrière l'Allemagne (6 109 noms) et juste devant les Pays-Bas (2 328 noms).

Le 7 avril prochain, les citoyens européens pourront donc avoir leur nom de domaine .EU, selon la règle « premier arrivé, premier servi » !

Avant d'enregistrer votre nom de domaine européen, il sera toutefois indispensable de vérifier sa disponibilité, puisque certains noms sont d'ores et déjà validés et actifs. Actuellement, INDOM (registrar français – www.indom.com) propose un moteur de vérification de disponibilité fonctionnel sur le .EU. Cet outil permet de visualiser les noms de domaine encore libres et de vérifier qu'un nom potentiellement gênant pour vous, votre activité ou votre société n'a pas déjà été déposé.

A noter que la liste des noms de domaine déposés mais refusés par l'agent de validation lors des deux périodes « sunrise »[2] sera publiée dans le courant du mois de juin 2006. Ils seront alors attribués selon la règle « premier arrivé, premier servi ».

A partir du 20 juin prochain, à 9h du matin, les

particuliers français pourront eux aussi déposer un nom de domaine en .FR.

Pour l'instant, selon les règles de l'AFNIC[3] en vigueur, seules les sociétés, les organismes publics, les associations ou les titulaires d'une marque française peuvent enregistrer un nom de domaine en .FR.

Le 20 juin, toute personne majeure et disposant d'une adresse postale en France pourra enfin devenir titulaire d'un nom de domaine en .FR, selon la règle « premier arrivé, premier servi ». Encore faut-il qu'il soit disponible, qu'il ne porte pas atteinte à des droits antérieurs (marques, raisons sociales, noms commerciaux...), ou à une personne et qu'il ne soit pas attentatoire à l'ordre public, aux mœurs, à une religion ou une race. L'AFNIC tient à jour une liste des termes interdits, exclus du nommage par nature ou déjà réservés. Une liste des noms des communes, dont l'enregistrement est soumis à une procédure spécifique, est quant à elle disponible sur le site de l'INSEE[4].

L'enregistrement en ligne sera alors possible sans fournir de document, sous réserve d'une vérification ultérieure par l'AFNIC de l'éligibilité du postulant.

Nicolas Samarcq, Juriste TIC, www.lexagone.com
Patrick Hauss, Indom Europe, www.indom.com

Par M. Nicolas Samarcq, Juriste TIC et M. Patrick Hauss

---

[1] Phase d'enregistrement préférentiel de deux mois ouverte aux titulaires de marques nationales et communautaires enregistrées, aux organismes publics et aux indications géographiques et appellations d'origine.

[2] Phase d'enregistrement préférentiel. La seconde période « sunrise », du 7 février au 7 avril à 11h, est ouverte aux titulaires de noms commerciaux, noms de sociétés et titres distinctifs des œuvres littéraires et artistiques protégées.

[3] Organisme chargé de la gestion administrative et technique des noms de domaine en *.fr* (France) et *.re* (Île de la Réunion).

[4] http://www.insee.fr/fr/nom_def_met/nomenclatures/cog/cog.telechargement.asp.

DROIT-TIC .com

R.D.T.I.C

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

PROPRIÉTÉS INTELLECTUELLES, DROIT D'AUTEUR

DROITS D'AUTEUR : LA DIFFICILE ADAPTATION À L'ÈRE DU NUMÉRIQUE

Par M. Nicolas Samarcq, Juriste TIC

En urgence déclarée, plus de deux ans après son dépôt à l'Assemblée nationale, le projet de loi sur le « *droit d'auteur, droits voisins dans la société de l'information* » (DADVSI) a été adopté, en première lecture, par les députés, le 21 mars dernier. Revue de l'essentiel.

Rejet de la licence globale optionnelle

L'article 1er du projet de loi instaurant la licence globale optionnelle (amendements PS et UMP du 21 décembre 2005), contre l'avis du gouvernement, avait contraint le ministre la culture de suspendre pendant deux mois et demi l'examen du texte pour présenter une nouvelle mouture. Le 6 mars, à la veille de la reprise des travaux parlementaires, cet article fut retiré par un amendement du gouvernement. Ce n'est que sous la menace d'une censure du Conseil constitutionnel, qui aurait lui même alerté le gouvernement, que le ministre a réintroduit l'article 1er dans sa rédaction de décembre 2005. Après tant de volte-face, l'Assemblée nationale, en l'absence des députés PS, PCF, Verts et UDF qui avaient quitté l'hémicycle en signe de protestation, a finalement décidé d'écarter la licence globale optionnelle.

Les nouvelles exceptions

L'article 1er bis du projet de loi prévoit désormais quatre nouvelles exceptions aux droits patrimoniaux de l'auteur (*art. L. 122-5 du Code de la Propriété Intellectuelle*).

Conformément à la directive européenne du 22 mai 2001 (dont la transposition devait intervenir au plus tard le 22 décembre 2002 !), ces exceptions visent :

- Les reproductions provisoires à caractère transitoire ou accessoire nécessaires à la transmission ou l'utilisation licite des œuvres sur internet (*routing, caching, browsing*, *streaming*).

- Les reproductions et représentations effectuées par des personnes morales et tous les établissements ouverts au public[1] en vue d'une consultation strictement personnelle des œuvres au profit des personnes souffrant d'un handicap supérieur à 50 %.

- Les reproductions effectués par les bibliothèques, les musées et les services d'archives qui ne recherchent aucun avantage commercial ou économique direct ou indirect et qui visent les actes nécessaires à l'accomplissement de leurs missions.

- Les reproductions intégrales ou partielles par voie de presse (écrite, audiovisuelle ou en ligne) des œuvres d'art graphiques, plastiques ou architecturales dans un but d'information, sous réserve d'indiquer le nom de l'auteur et la source, à moins que cela s'avère impossible.

L'ensemble des exceptions de l'article L. 122-5 du Code de la propriété intellectuelle (copie privée, analyse et courte citation, revue de presse, parodie, pastiche et caricature, …) sont soumises au *test en trois étapes*. Autrement dit, elles ne doivent pas « *porter atteinte à l'exploitation normale de l'œuvre ni causer un préjudice injustifié aux intérêts légitimes de l'auteur*».

Les mesures techniques de protection (MTP)

Les MTP, consacrées quelques jours avant la reprise des débats parlementaires par la Cour de cassation dans l'affaire « *Mulholland drive* » »[2], seront désormais encadrés par la loi afin de garantir les droits de chacun.

Selon le projet de loi, les MTP sont destinées à empêcher ou limiter les utilisations non autorisées par le titulaire d'un droit d'auteur ou d'un droit voisin d'une œuvre (autre qu'un logiciel), d'une interprétation, d'un phonogramme, d'un vidéogramme ou d'un programme.

Les logiciels susceptibles de traiter des œuvres protégées et intégrant des MTP permettant le contrôle à distance direct ou indirect d'une ou plusieurs fonctionnalités, ou l'accès à des données personnelles, sont soumis à une procédure de déclaration préalable auprès des services de l'État en charge de la sécurité des systèmes d'information. En cas de traitements de données personnelles, le responsable des traitements devra aussi respecter les obligations de loyauté et de sécurité de la loi Informatique et Libertés.

Les MTP ne doivent pas avoir pour effet d'empêcher la mise en œuvre effective de l'interopérabilité. Récemment l'ADAMI, qui gère les droits de propriété littéraire et artistique des artistes-interprètes pour l'utilisation de leur travail enregistré a dénoncé l'incompatibilité des formats de compression et des DRM[3]. Actuellement, les utilisateurs de lecteurs compressés ne peuvent accéder à l'ensemble des plates-formes commerciales. Ainsi, le WMA (*Windows media audio*) de Microsoft, adopté par les plates-formes de téléchargement OD2, Fnac, Virgin, ne peut être lu par l'iPod d'Apple (40% des ventes), iTunes Music Store, le site de téléchargement d'Apple, est compatible avec les seuls iPod et Hewlett Packard Look Like et les téléchargements sur le site de Sony Music ne sont possibles que sur les baladeurs de la marque.

Les fournisseurs de MTP auront donc l'obligation de donner accès aux informations essentielles permettant la compatibilité de leurs systèmes de lecture. Les actes de décompilation nécessaires à l'obtention de ces informations seront autorisés. En cas de défaillance dans la fourniture de ces données, tout intéressé pourra saisir le président du tribunal de grande instance, en référé, pour en obtenir communication.

Apple a déjà réagi en accusant l'Etat français de vouloir « *parainer le piratage* ». En réalité, cette disposition française remet en cause le modèle économique de sa plate-forme iTunes, d'ailleurs sous le coup d'une enquête de la Commission européenne au Royaume-Uni, depuis février 2005. Jonathan Todd, porte-parole de la Commissaire européenne à la concurrence, précise toutefois que cette procédure porte *sur les divergences de prix* et non sur les mesures de verrouillage. Outre-manche, chaque titre de musique est vendu 79 pennies (1,14 euros) et les internautes britanniques ne sont pas autorisés à acheter des titres sur les autres plates-formes iTunes européennes.

Le projet vise également à garantir le « *droit au bénéfice de l'exception pour copie privée* » par la création d'un collège de médiateurs qui aura pour mission de fixer, en fonction du type d'œuvre ou de support, les modalités d'exercice de l'exception et de réguler les mesures techniques.

Dans un délai raisonnable, les titulaires de droits auront l'obligation de mettre en œuvre des MTP qui permettront le bénéfice effectif des exceptions précitées.

Toute limitation de la lecture d'une œuvre résultant de MTP devra faire l'objet d'une information de l'utilisateur. Les modalités de cette information seront fixées par décret en Conseil d'État.

Téléchargements et mises à disposition illicites

Le nouveau dispositif écarte les sanctions pénales pour les actes de contrefaçon des particuliers réalisés à des fins personnelles et non commerciales.

Dans cette hypothèse, les actes de téléchargement seront passibles d'une amende de 1ère classe (38 euros) et les opérations de mise à disposition au public d'une contravention de 2ème classe (150 euros).

Les cas de téléchargements et de mises à disposition illicites à titre commercial sont punis de trois ans de prison et 300 000 euros maximum.

Logiciels P2P

Le fait d'éditer ou de mettre disposition sciemment un « *dispositif* » manifestement destiné à la mise à disposition non autorisée d'œuvres ou d'objets protégés sera passible de trois ans d'emprisonnement et de 300 000 euros d'amende. Cette peine sera également encourue par la personne qui incite, y compris a travers une annonce publicitaire, à l'usage d'un tel logiciel.

En référé, le juge pourra ordonner aux éditeurs de logiciels permettant « *l'acquisition illicite* » d'œuvres et « *manifestement utilisés à une échelle commerciale* », de prendre des mesures pour empêcher ou limiter ces usages illicites, lorsque cela ne remet pas en cause la destination initiale du logiciel.

JURISPRUDENCES

C. Cass., Ch. Crim., 14 mars 2006, FABRICE H. C/ MINISTÈRE PUBLIC

Thèmes
Informatique et libertés, Pourriel, spam, courriel, vie privée

Abstract
Données à caractère personnel, collecte, conservation des information (non), information des personnes (non), courriel, envoi non sollicité / pourriel (oui), collecte déloyale (oui)
Résumé
un prévenu est condamné sur le fondement de la collecte déloyale pour avoir utilisé et proposé à la vente un progiciel permettant d'adresser des messages non sollicités grâce aux adresses disponibles dans les espaces publics, sans les conserver.

Décision

COUR DE CASSATION, chambre criminelle, 14 mars 2006 Fabrice H. c/ Ministère public
N° F 05-83423 F-P+F – Rejet

REPUBLIQUE FRANCAISE

AU NOM DU PEUPLE FRANCAIS

LA COUR DE CASSATION, CHAMBRE CRIMINELLE, en son audience publique tenue au Palais de Justice à PARIS, le quatorze mars deux mille six, a rendu l'arrêt suivant :

Sur le rapport de M. le conseiller référendaire VALAT, les observations de Me SPINOSI, avocat en la Cour, et les conclusions de M. l'avocat général CHARPENEL ;

Statuant sur le pourvoi formé par Fabrice H. contre l'arrêt de la cour d'appel de PARIS, 11e chambre, en date du 18 mai 2005, qui, pour collecte de données nominatives par un moyen frauduleux, déloyal ou illicite, l'a condamné à 3 000 euros d'amende ;

Vu le mémoire produit ;

Sur le moyen unique de cassation, pris de la violation des articles 226-18 du Code pénal, 25 et 41 de la loi du 6 janvier 1978, 7 de la directive communautaire du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement de données à caractère personnel et à la libre circulation de ces données, 591 et 593 du Code de procédure pénale ;

« *en ce que la cour d'appel a déclaré le prévenu coupable du délit de collecte de données nominative aux fins de constituer des fichiers ou des traitements informatiques par un moyen frauduleux, déloyal ou illicite ;*

aux motifs qu'il est reproché à Fabrice H. d'avoir, entre avril 2002 et le 20 octobre 2002, collecté des données nominatives concernant des personnes physiques par l'utilisation des logiciels "Robot Mail" et "Freeprospect", aux fins de constituer des fichiers ou des traitements informatiques, par un moyen frauduleux, déloyal ou illicite ; que le délit de l'article 226-18, alinéa 1er, du Code pénal suppose, pour être constitué, qu'il y ait collecte, selon un traitement automatisé, de données nominatives par un moyen frauduleux, déloyal ou illicite ; qu'il est constant que Fabrice H. a mis en œuvre les logiciels "Robot Mail" et "Freeprospect" permettant d' "aspirer", sur internet, des adresses électroniques de personnes physiques en vue de la diffusion de messages publicitaires aux titulaires de ces adresses ; que sur les faits relatifs au logiciel "Robot Mail" : qu'il n'est pas contesté qu'à partir du 13 avril 2002, des spams, expédiés par une personne dont l'adresse électronique était "fabriceh@aol.com", ont été reçus par des internautes personnes physiques par suite de l'emploi, par la société ABS, du logiciel "Robot Mail" ; que, comme l'ont indiqué les premiers juges, les adresses électroniques collectées constituent des données nominatives au sens de l'article 4 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés dès lors qu'elles permettent l'identification des personnes physiques auxquelles elles s'appliquent, ce que ne conteste d'ailleurs pas le prévenu ; qu'il n'est pas discuté que le logiciel "Robot Mail" permettait de capturer et de traiter les données collectées qu'il conservait dans un fichier, ainsi que l'admet Fabrice H. ; que ces opérations sont en conséquence constitutives d'une collecte de données au sens de l'article 226-18 du Code pénal ; que, si la collecte a été assurée par la capture d'informations diffusées sur des sites publics - sites Web, annuaires, forums de discussion - il n'en demeure pas moins qu'elle a été opérée par un moyen illicite, et en tout cas déloyal, en ce que : - les adresses collectées sur des sites ou annuaires professionnels ou sur des forums de discussion ont en l'espèce donné lieu à une utilisation sans rapport avec l'objet de leur mise en ligne ;

- le consentement des personnes titulaires de ces adresses n'a à aucun moment été recueilli alors que : - ces personnes disposaient, en vertu de l'article 26 de la loi du 6 janvier 1978 dans sa rédaction en vigueur à la

date des faits, d'un droit d'opposition supposant qu'elles soient avisées, préalablement à leur inscription sur un fichier, de ce que des informations nominatives les concernant étaient susceptibles de faire l'objet d'un traitement ;

- l'article 7 de la directive communautaire n° 95/46/CE du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, alors en vigueur, dispose que les Etats membres prévoient que "le traitement de données à caractère personnel ne peut être effectué que si la personne concernée a indubitablement donné son consentement", le consentement étant défini par l'article 2 du texte comme "la manifestation de volonté, libre, spécifique et informée par laquelle la personne concernée accepte que les données à caractère personnel la concernant fassent l'objet d'un traitement" ;

- Fabrice H., professionnel avisé de l'informatique, ne pouvait méconnaître l'ensemble des dispositions applicables en la matière ;

que Fabrice H. reconnaît implicitement que ce logiciel n'était pas conforme aux règles applicables puisqu'il en a interrompu la vente le 20 octobre 2002 ; que dans ces circonstances, l'infraction de collecte de données nominatives par un moyen illicite ou déloyal en ce qui concerne le logiciel "Robot Mail" est pleinement constituée à l'encontre du prévenu pour la période comprise entre avril 2002 et le 20 octobre 2002 ; que la Cour déclarera en conséquence Fabrice H. coupable de cette infraction et infirmera en ce sens le jugement déféré ;

sur les faits relatifs au logiciel "Freeprospect" : que Fabrice H. conteste pas sérieusement que des spams ont été reçus par des intemautes personnes physiques à partir d'octobre 2002 par suite de l'emploi du logiciel "Freeprospect", le prévenu ayant admis que ce logiciel, s'il vise les sites professionnels, a néanmoins pu, en dépit des vérifications opérées par ses soins, cibler des sites de particuliers ; que le prévenu fait valoir que le logiciel "Freeprospect" ne capture aucune information et ne procède à aucun enregistrement de données, se bornant à cibler directement l'adresse électronique concernée à laquelle est envoyée instantanément le courrier publicitaire, et qu'il n'y a donc pas ici de collecte d'information nominative ; que, lors de son audition du 1er septembre 2003, Fabrice H. a reconnu qu'il y avait bien eu en l'espèce collecte de données ; qu'en outre le délit prévu et puni par l'article 226-18, alinéa 1er, du Code pénal suppose une collecte et un traitement d'informations, sans se limiter à l'enregistrement de données ; que ces deux éléments de collecte et de traitement sont bien réunis en l'espèce, le logiciel "Freeprospect" ayant précisément pour fonction à la fois de collecter des informations et de les traiter instantanément, étant observé qu'en tout état de cause le système informatique de l'opérateur mémorise nécessairement ne serait-ce qu'un instant infime sur la mémoire vive, l'adresse concernée pour permettre l'envoi du message, comme l'a d'ailleurs admis Fabrice H. lors de son audition du 1er septembre 2003 ; qu'ainsi que la Cour l'a observé plus haut pour le logiciel "Robot Mail", la capture des informations en cause a ici été opérée par un moyen illicite, et en tout cas déloyal, à la fois par le détournement des adresses mises en ligne et par l'absence de consentement au traitement des personnes titulaires de ces adresses, alors que : - le prévenu ne rapporte pas la preuve qu'au cours de la période visée à la prévention, les titulaires d'adresses concernées aient effectivement donné leur consentement préalable et certain à l'utilisation de leur adresse électronique, ni aient été mis en mesure de s'opposer au traitement des données ; - les internautes entendus dans le cadre de l'enquête préliminaire ont indiqué que les messages adressés par la société ABS soit ne comprenaient toujours pas de lien hypertexte de demande de consentement, soit comportaient unlien de désabonnement mais hors d'état de fonctionnement ; - Fabrice H. a reconnu l'existence de dysfonctionnements dans la mise en œuvre des procédures ; - au surplus, les documents produits par le prévenu au soutien de l'existence d'un lien de désinscription démontrent que les adresses électroniques des intemautes étaient bien utilisées a priori, les propositions de désinscription n'étant en tout état de cause envoyées aux personnes concernées que dans un second temps ; qu'il établi que le logiciel "Freeprospect" a été commercialisé et utilisé entre octobre 2002 et le 1er septembre 2003 ; que Fabrice H. ne saurait ici invoquer sa bonne foi dès lors qu'il était pleinement informé des dispositions légales applicables et qu'il avait connaissance, en particulier dans le cadre des nombreux échanges intervenus avec la CNIL, des difficultés rencontrées sur la question du consentement des titulaires d'adresses électroniques ; qu'il est, dans ces circonstances, suffisamment établi que Fabrice H. a procédé, en ce qui concerne le logiciel "Freeprospect", à la collecte de données nominatives par un moyen illicite ou déloyal ; que la Cour déclarera en conséquence Fabrice H. coupable de cette infraction et infirmera eu ce sens le jugement déféré» ;

"alors que, d'une part, compte tenu de l'accessibilité universelle de l'Internet, l'identification et même la collecte, sans le consentement des intéressés, d'adresses électroniques, non pas utilisées lors de communications privées, mais figurant sur l'espace public de l'Internet, tel que les sites web, les annuaires ou les forum de discussion, n'implique l'usage d'aucun procédé frauduleux, déloyal ou illicite ;

"alors que, d'autre part, en imposant, pour qu'une collecte de données nominative ne soit pas illicite, le consentement nécessaire de chaque personne concernée par les informations collectées, la cour d'appel a ajouté au texte de l'article 226-18 du Code pénal une

condition qu'il ne contient pas en méconnaissance du principe de l'interprétation stricte de la loi pénale ;

"alors qu'en outre, le seul fait pour un logiciel de cibler une adresse électronique pour lui envoyer un courrier sans que cette information ne soit ni enregistrée, ni visible, ni conservée, ne peut constituer une collecte d'information nominative ; qu'en retenant pourtant que le délit puni par l'article 226-18 du Code pénal supposait une collecte et un traitement informatique sans se limiter à l'enregistrement de données, la cour d'appel à méconnu le sens et la portée de cette disposition légale" ;

Attendu qu'il résulte de l'arrêt attaqué et des pièces de procédure que la société Alliance bureautique service (ABS) a adressé, en 2002 et 2003, des courriers électroniques publicitaires non sollicités à des particuliers dont elle avait obtenu les adresses électroniques sur l'espace public du réseau internet en utilisant, dans un premier temps, le logiciel Robot mail qui enregistrait ces informations dans un fichier en vue d'un usage ultérieur puis, dans un second temps, à l'aide du logiciel Freeprospect qui adressait les messages publicitaires aux adresses collectées sans les enregistrer dans un fichier ; que, sur dénonciation de la Commission nationale de l'informatique et des libertés, Fabrice H., dirigeant de la société ABS, a été cité par le procureur de la République devant la juridiction correctionnelle du chef de collecte de données nominatives par un moyen frauduleux, déloyal ou illicite ; qu'il a été renvoyé des fins de la poursuite ; que le ministère public a interjeté appel ;

Attendu que, pour déclarer le prévenu coupable du délit prévu par l'article 226-18 du Code pénal dans sa rédaction alors en vigueur et le condamner, l'arrêt attaqué énonce qu'il a collecté des adresses électroniques, qui constituent des données nominatives, de façon déloyale en ce qu'elles ont été utilisées sans rapport avec l'objet de leur mise en ligne ; que les juges ajoutent que les titulaires des adresses n'ont pas donné leur consentement alors que le droit d'opposition dont ils disposaient supposait qu'ils soient avisés, avant tout enregistrement, de ce que les informations nominatives les concernant pouvaient faire l'objet d'un traitement ; qu'enfin, pour écarter l'argumentation du prévenu qui faisait valoir que le logiciel Freeprospect se bornait à cibler l'adresse électronique concernée, mais n'enregistrait aucune donnée, les juges retiennent que les données sont collectées et traitées et que les adresses sont mémorisées ne serait-ce qu'un instant dans la mémoire vive de l'ordinateur ;

Attendu qu'en cet état, la cour d'appel a justifié sa décision ;

Que, d'une part, constitue une collecte de données nominatives le fait d'identifier des adresses électroniques et de les utiliser, même sans les enregistrer dans un fichier, pour adresser à leurs titulaires des messages électroniques ;

Que, d'autre part, est déloyal le fait de recueillir, à leur insu, des adresses électroniques personnelles de personnes physiques sur l'espace public d'internet, ce procédé faisant obstacle à leur droit d'opposition ;

D'où il suit que le moyen doit être écarté ;

Et attendu que l'arrêt est régulier en la forme ;

REJETTE le pourvoi ;

Ainsi jugé et prononcé par la Cour de cassation, chambre criminelle, en son audience publique, les jour, mois et an que dessus ;

Etaient présents aux débats et au délibéré : M. Cotte président, M. Valat conseiller rapporteur, M. Joly, Mme Anzani, MM. Beyer, Pometan, Mmes Palisse, Guirimand, M. Beauvais, Mme Ract-Madoux conseillers de la chambre, Mme Ménotti conseiller référendaire ;

Avocat général : M. Charpenel ;

Greffier de chambre : Mme Randouin ;

En foi de quoi le présent arrêt a été signé par le président, le rapporteur et le greffier de chambre ;

Référence : C. Cass., Ch. Crim., 14 mars 2006, *FABRICE H. C/ MINISTÈRE PUBLIC*, DROIT-TIC http://www.droit-tic.com/juris/aff.php?id_juris=73

R.D.T.I.C
LA REVUE DU DROIT DES TECHNIQUES DE L'INFORMATION ET DE LA COMMUNICATION

CA Paris, 11ème Ch., 18 mai 2005, FABRICE H. / MINISTÈRE

Thèmes
Pourriel, spam, courriel, vie privée, Droit de la consommation, protection du consommateur

Abstract
Données à caractère personnel, collecte, conservation des information, information des personnes (non), courriel, envoi non sollicité / pourriel (oui), collecte déloyale (oui)
Résumé
un prévenu est condamné sur le fondement de la collecte déloyale pour avoir utilisé et proposé à la vente un progiciel permettant d'adresser des messages non sollicités grâce aux adresses disponibles dans les espaces publics, sans les conserver

Décision

Extraits

(...)

Au cours de l'année 2002, la CNIL a été informée que de nombreux messages publicitaires – spams- étaient adressés à la société Alliance Bureautique Service (ABS), ayant pour gérant F.H avec laquelle ils n'avaient à aucun moment été mis en contact.

Le 22 janvier 2003, le président de la CNIL a dénoncé au procureur de la République près le tribunal de grande instance de Paris l'utilisation et la commercialisation par la société ABS de deux logiciels « Robot mail » et « Feeprospect », utilisés pour la collecte d'adresses informatiques et la diffusion de spams aux titulaires des ces adresses.

Par le jugement déféré, le tribunal correctionnel a renvoyé F.H du chef de collecte de données nominatives par un moyen frauduleux, illicite ou déloyal pour l'emploi des logiciels « Robot Mail » et « Freeprospect », estimant que les collectes des données opérées à l'aide de ces deux logiciels ne présentaient aucun caractère frauduleux, illicite ou déloyal.

(...)

Au fond

Considérant qu'il est reproché à F.H d'avoir, entre avril 2002 et le 20 octobre 2002, collecté des données nominatives concernant des personnes physiques par l'utilisation des logiciels « Robot Mail » et « Freeprospect », aux fins de constituer des fichiers ou des traitements informatiques, par un moyen frauduleux, illicite ou déloyal ;

Considérant que le délit de l'article 226-18 alinéa 1 er du code pénal suppose, pour être constitué, qu'il y ait collecte, selon un traitement automatisé, de données nominatives par un moyen caractère frauduleux, illicite ou déloyal ;

Considérant qu'il est constant que F.H a mis en œuvre les logiciels « Robot Mail » et « Freeprospect » permettant « d'aspirer », sur internet, des adresses de messagerie électroniques de personnes physiques en vue de la diffusion de messages publicitaires aux titulaires de ces adresses ;

Sur les faits relatifs au logiciel « Robot Mail »

Considérant qu'il n'est pas contesté qu'à partir du 13 avril 2002, des spams expédiés par une personne dont l'adresse électronique était « F.H@aol.com », ont été reçus par des internautes personnes physiques par suite de l'emploi, par la société ABS, du logiciel « Robot Mail » ;

Considérant que, comme l'ont indiqué les premiers juges, les adresses électroniques collectées constituent des données nominatives au sens de l'article 4 de la loi n° 78-17 du 6 janvier 1978 dès lors qu'elles permettent l'identification des personnes physiques auxquelles s'appliquent, ce que ne conteste d'ailleurs pas le prévenu ;

Considérant qu'il n'est pas discuté que le logiciel « Robot Mailé permettait de capturer et de traiter les données collectées qu'il conservait dans un fichier, ainsi que l'admet F.H ; que cers opérations sont en conséquence constitutives d'une collecte de données au sens de l'article 226-18 du code pénal.

Considérant que si la collecte a été assurée par la capture d'informations diffusées sur des sites publics – sites web, annuaires, forums de discussion- il n'en demeure pas moins qu'elle a été opérée par un moyen illicite, en tout cas déloyal, en ce que :

- Les adresses collectées sur des sites ou annuaires professionnels ou sur des forums de discussion ont en l'espèce donné lieu à une tulisation sans rapport avec l'objet de leur mise en ligne ;

- le consentement des personnes titulaires de ces adresses n'a à aucun moment été recueillie alors que :

- ces personnes disposaient, en vertu d l'article 26 de la loi du 6 janvier 1978 d'un droit d'opposition supposant qu'elles soient avisées préalablement à leur inscription sur un fichier, de ce que des informations nominatives les concernant étaient susceptibles de faire l'objet d'un traitement ;

- l'article 7 de la directive communautaire n° 95/46/CE du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, alors en vigueur, dispose que les Etats membres prévoient que "le traitement de données à caractère personnel ne peut être effectué que si la personne concernée a indubitablement donné son consentement", le consentement étant défini par l'article 2 du texte comme "la manifestation de volonté, libre, spécifique et informée par laquelle la personne concernée accepte que les données à caractère personnel la concernant fassent l'objet d'un traitement" ;

- Fabrice H., professionnel avisé de l'informatique, ne pouvait méconnaître l'ensemble des dispositions applicables en la matière ;

que Fabrice H. reconnaît implicitement que ce logiciel n'était pas conforme aux règles applicables puisqu'il en a interrompu la vente le 20 octobre 2002 ; que dans ces circonstances, l'infraction de collecte de données nominatives par un moyen illicite ou déloyal en ce qui concerne le logiciel "Robot Mail" est pleinement constituée à l'encontre du prévenu pour la période comprise entre avril 2002 et le 20 octobre 2002 ; que la Cour déclarera en conséquence Fabrice H. coupable de cette infraction et infirmera en ce sens le jugement déféré ;

Sur les faits relatifs au logiciel « Freeprospect »

Considérant que Fabrice H. conteste pas sérieusement que des spams ont été reçus par des intemautes personnes physiques à partir d'octobre 2002 par suite de l'emploi du logiciel "Freeprospect", le prévenu ayant admis que ce logiciel, s'il vise les sites professionnels, a néanmoins pu, en dépit des vérifications opérées par ses soins, cibler des sites de particuliers ;

Considérant que le prévenu fait valoir que le logiciel "Freeprospect" ne capture aucune information et ne procède à aucun enregistrement de données, se bornant à cibler directement l'adresse électronique concernée à laquelle est envoyée instantanément le courrier publicitaire, et qu'il n'y a donc pas ici de collecte d'information nominative ;

Mais considérant que, lors de son audition du 1er septembre 2003, Fabrice H. a reconnu qu'il y avait bien eu en l'espèce collecte de données ;

qu'en outre le délit prévu et puni par l'article 226-18, alinéa 1er, du Code pénal suppose une collecte et un traitement d'informations, sans se limiter à l'enregistrement de données ;

Considérant que ces deux éléments de collecte et de traitement sont bien réunis en l'espèce, le logiciel "Freeprospect" ayant précisément pour fonction à la fois de collecter des informations et de les traiter instantanément, étant observé qu'en tout état de cause le système informatique de l'opérateur mémorise nécessairement ne serait-ce qu'un instant infime sur la mémoire vive, l'adresse concernée pour permettre l'envoi du message, comme l'a d'ailleurs admis Fabrice H. lors de son audition du 1er septembre 2003 ;

Considérant ainsi que la Cour l'a observé plus haut pour le logiciel "Robot Mail", la capture des informations en cause a ici été opérée par un moyen illicite, et en tout cas déloyal, à la fois par le détournement des adresses mises en ligne et par l'absence de consentement au traitement des personnes titulaires de ces adresses, alors que :

- le prévenu ne rapporte pas la preuve qu'au cours de la période visée à la prévention, les titulaires d'adresses concernées aient effectivement donné leur consentement préalable et certain à l'utilisation de leur adresse électronique, ni aient été mis en mesure de s'opposer au traitement des données ;

- les internautes entendus dans le cadre de l'enquête préliminaire ont indiqué que les messages adressés par la société ABS soit ne comprenaient toujours pas de lien hypertexte de demande de consentement, soit comportaient un lien de désabonnement mais hors d'état de fonctionnement ;

- Fabrice H. a reconnu l'existence de dysfonctionnements dans la mise en œuvre des procédures ;

- au surplus, les documents produits par le prévenu au soutien de l'existence d'un lien de désinscription démontrent que les adresses électroniques des intemautes étaient bien utilisées a priori, les propositions de désinscription n'étant en tout état de cause envoyées aux personnes concernées que dans un second temps ;

qu'il établi que le logiciel "Freeprospect" a été commercialisé et utilisé entre octobre 2002 et le 1er septembre 2003 ;

que Fabrice H. ne saurait ici invoquer sa bonne foi dès lors qu'il était pleinement informé des dispositions légales applicables et qu'il avait connaissance, en particulier dans le cadre des nombreux échanges intervenus avec la CNIL, des difficultés rencontrées sur la question du consentement des titulaires d'adresses électroniques ;

qu'il est, dans ces circonstances, suffisamment établi que Fabrice H. a procédé, en ce qui concerne le logiciel "Freeprospect", à la collecte de données nominatives par un moyen illicite ou déloyal ;

que la Cour déclarera en conséquence Fabrice H. coupable de cette infraction et infirmera eu ce sens le jugement déféré

(…)

Référence : CA de Paris, 11ème Ch., 18 mai 2005, *FABRICE H. / MINISTÈRE PUBLIC*, DROIT-TIC
http://www.droit-tic.com/juris/aff.php?id_juris=74

DROIT-TIC .com

R.D.T.I.C

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

T. Corr. Paris, 17ème Chambre, 7 décembre 2004, MINISTÈRE PUBLIC C/ FABRICE H.

Thèmes
Informatique et libertés, Pourriel, spam, courriel, vie privée

Abstract
Droit des personnes - informatique et Libertés - publipostage électronique / spam - logiciel aspirateur d'asresse électronique - collecte déloyale (non).

Résumé
La collecte des adresses électroniques disponibles sur les espaces publiques de l'Internet sans information prélable est reconnu loyale sous l'empire de la la loi 78/17 du 6 janvier 1978. Faits antérieurs à la modification du 6 aout 2004.

Décision

EXTRAIT DE LA DECISION

"Les faits

La commission nationale de l'informatique et des libertés (CNIL) a adopté le 24 octobre 2002 une délibération n° 02-075, dans laquelle elle rappelle que, suite à un précédent rapport sur "le publipostage électronique et la protection des données personnelles" adopté en octobre 1999, elle a mis en place, au mois de juillet 2002, une boite à lettre électronique (accessible à l'adresse spam@cnil.fr) spécialement destinée à recueillir les courriers électroniques non sollicités (souvent désignés par le terme anglais de spam, de même que l'envoi de tels courriers est dénommé spamming) reçus par les utilisateurs du réseau internet et transférés par eux.

La délibération rappelle la définition donnée par la CNIL elle-même de cette pratique dite de spamming : "l'envoi massif -et parfois répété- de courriers électroniques non sollicités, le plus souvent à caractère commercial, à des personnes avec lesquelles 1'expéditeur n 'a jamais eu de contact et dont il a capté 1'adresse dans les espaces publics de l'internet : forums de discussion, listes de diffusion, annuaires, sites web. etc. ".

Elle fait ensuite état des nombreux courriels reçus à l'adresse précitée et transférant des courriers électroniques émanant de la société ALLIANCE BUREAUTIQUE SERVICE (ABS) proposant à la vente un outil informatique dénommé robotmail et permettant à ses utilisateurs de collecter des adresses électroniques dans les espaces publics de l'internet et de se constituer ainsi des fichiers de prospects. Estimant cette pratique contraire à la loi n° 78-17 du 6 janvier 1978 (dite informatique et libertés), la commission décidait de dénoncer au parquet des faits susceptibles de caractériser les infractions pénales des articles 226-16 et 226-18 du code pénal.

S'il ne résulte pas du dossier que cette délibération ait, à cette date, été transmise au parquet, le procureur de la République près ce tribunal a, en revanche, été ultérieurement destinataire de deux courriers qui lui ont été adressés par le président de la CNIL, les 22 janvier (dénonciation de l'utilisation et de la commercialisation, par la même société, d'un nouveau logiciel dénommé freeprospect) et 11 février 2003 (transmission d'une saisine émanant d'un client mécontent de la société ABS, qui avait acheté le logiciel robotmail, l'Institut de REIKI, association de formation professionnelle pour adultes qui avait déjà directement saisi le parquet le 21 novembre précédent des mêmes faits et a, depuis, retiré sa plainte le 29 juin 2003).

Le ministère public a ordonné, à la suite de ces différentes transmissions, deux enquêtes, qui ont été jointes et au vu desquelles il a décidé des poursuites dont ce tribunal est présentenïent saisi.

Les deux logiciels litigieux n'ont pas fait l'objet, dans le cadre de ces investigations, d'une analyse et d'une description rigoureuses. Il résulte de la procédure et des débats qu'ils permettent, tous les deux, la collecte d'adresses électroniques (comportant le symbole @) disponibles sur des sites dont la sélection est effectuée sur la base des objectifs commerciaux prédéterminés par leur utilisateur, de sorte à permettre l'envoi aux dites adresses de messages à caractère publicitaires. Il n'est pas contesté que le logiciel robotmail, le premier mis au point par la société ABS -société dont le prévenu, Fabrice H, est le principal animateur-, après avoir collecté ces adresses, les stocke, afin qu'elles puissent être utilisées pour l' expéditions des messages commerciaux propres à chacun de ses utilisateurs. Le logiciel freeprospect, mis au point ultérieurement. pour éviter les critiques adressées à l'outil précédent, et disponible à partir de l'automne 2002, collecte, selon un principe proche, des adresses sans cependant les stocker mais en les utilisant au fur et à mesure de leur collecte pour l'expédition des mêmes propositions commerciales.

Les personnes recevant une prospection adressée par le biais de ces logiciels devaient se voir offrir la possibilité de refuser tout nouvel envoi. Un lien de désinscription était normalement prévu à cet effet et, s'agissant du logiciel freeprospect, un premier envoi préalable devait permettre â celui qui le recevait d'accepter ou non de se voir adresser des propositions commerciales. Il résultait de nombre des signalements adressés à la CNIL que ces systèmes n'avaient fonctionné que très rarement, le

prévenu ne contestant pas l'existence, pour des raisons techniques, de dysfonctionnements les ayant souvent privés de la moindre efficacité.

Seul le logiciel robotmail a fait l'objet, en date du 15juillet 2002, de la déclaration à la CNIL imposée par la loi de 1978 pour tout traitement automatisé d'informations nominatives. Le récépissé de cette déclaration a été adressé au mois de septembre 2002.

Le prévenu a expliqué au tribunal que l'utilisation de ces outils supposait une surveillance de la pertinence des sites intemet automatiquement sélectionnés, en fonction des critères requis par l'utilisateur, par un outil dénommé Copernic, afin de vérifier qu'il s' agissait de sites professionnels. et non de forums de discussions ou de pages personnelles, de telle sorte que les adresses électroniques collectées sur ces sites soient exclusivement de nature professionnelle. Il a indiqué que les consignes d'usage des deux logiciels litigieux précisaient ce point clairement.

Il a encore déclaré qu'il avait, à de nombreuses reprises, interrogé la CNIL sur le caractère licite de ces deux logiciels. Il justifie, à cet égard, de l'envoi de courriers à partir du mois d'août 2002. Il résulte, par ailleurs, des pièces produites par la commission, d'une part, que celle-ci avait interrogé la société ABS à la suite de réclamation d'internautes pour la première fois le 9 janvier 2002 et réclamé à plusieurs reprises une réponse à ses demandes d'explications et, d'autre part, que, le 15 octobre 2002, elle avait informé la société ABS de ce qu'elle considérait que la captation d'adresses électroniques dans les espaces publics de l'internet n' était pas licite et de ce qu' elle estimait qu'une opération de publipostage ne pouvait être régulière que si les personnes concernées avaient été informées de "l'usage commercial qui pourrait être fait à partir de leurs données personnelles et qu 'elles aient été mises en mesure de s'opposer préalablement à toute transmission de leurs données à des tiers".

Sur l'action publique

L'article 226-18 du code pénal, sur la base duquel sont engagées les présentes poursuites et qui sanctionne la violation de deux obligations différentes résultant de la loi du 6janvier 1978 en ses articles 25 et 26, prévoit et punit deux infractions distinctes : d'une part, "le fait de collecter des données par un moyen frauduleux, déloyal ou illicite" et, d'autre part, le fait de procéder à un traitement d'informations nominatives concernant une personne physique malgré l'opposition de cette personne, lorsque cette opposition est fondée sur des motifs légitimes".

La prévention combine ces deux infractions distinctes, de telle sorte que le tribunal doit l'examiner afin de déterminer si l'une ou l'autre de ces infractions ensemble poursuivies est constituée, en ne retenant, pour chacune d'elles, que les éléments constitutifs pertinents et visés dans l'acte saisissant le tribunal.

Les notions de données et de traitement d'informations nominatives doivent s'entendre au sens de la loi de 1978, en application des dispositions de l'article 41 de ce texte, qui précise que la section V du chapitre VI du titre II du livre II du code pénal, où est inséré l'article 226-18, a pour but de réprimer les infractions à cette loi.

Le premier délit réprimé par l'article 226-18 se réfère à l'interdiction, résultant de l'article 25 de la loi de 1978, de la collecte de données opérée par un moyen frauduleux, déloyal ou illicite et suppose donc, pour être constitué, la réunion de trois éléments distincts, une collecte, de données nominatives, par un moyen frauduleux, déloyal ou illicite.

Il résulte de l'article 4 de la loi que les données nominatives sont celles qui permettent, "sous quelque forme que ce soit, directement ou non l 'identification des personnes physiques auxquelles elles s'appliquent". Les adresses électroniques constituent, au sens de ce texte, des données nominatives, dès lors qu'elles permettent en règle générale d'identifier la personne physique auxquelles elles s'appliquent, soit directement, quand le nom et le prénom de cette personne figurent en toutes lettres dans l'adresse (cas des adresses expressément énumérées dans la prévention relative au logiciel robotmail), soit indirectement, lorsque des démarches auprès d'un intermédiaire technique sont nécessaires pour découvrir la personne physique titulaire de l'adresse concernée, et ceci, sauf les rares exceptions d'adresses génétiques de personnes morales, ne conduisant pas à une personne physique identifiable.

Le tribunal retient donc que les adresses collectées par les deux logiciels litigieux, telles qu'elles résultent de l'enquête effectuée, étaient, pour l'essentiel, des données nominatives.

Collecter des données signifie les recueillir et les rassembler, ce qui implique leur enregistrement ou leur conservation dans un fichier, II n'est pas contesté que le logiciel robotmail avait pour principe que les adresses électroniques collectées étaient regroupées dans un fichier, de façon à permettre l'expédition ultérieure de diverses propositions commerciales aux titulaires de ces adresses. Il n'en est pas de même s'agissant du logiciel freeprospect. II ne résulte d'aucun des éléments produits que les adresses collectées faisaient l'objet d'un stockage ou d'un enregistrement et ce fait, fermement contesté par le prévenu qui indique que chaque adresse détectée par le logiciel était immédiatement utilisée pour l'expédition d'un courriel, sans être enregistrée ni conservée, n'est d'ailleurs pas même allégué par l'accusation.

Cet élément constitutif de l'infraction manque donc, s'agissant du logiciel freeprospect.

Aucun des éléments de la cause ne permet, quoiqu'il en soit, au tribunal de retenir que la collecte à laquelle se livrait le logiciel robotmail avait un caractère déloyal, frauduleux ou illicite.

Le seul fait démontré et susceptible d'être pertinent à cet égard est que les titulaires des adresses ainsi rassemblées ignoraient,jusqu'à ce qu'ils reçoivent un courrier électronique envoyé grâce à ce système, que leurs adresses avaient été sélectionnées. Il convient à cet égard de relever que le consentement express des intéressés, qu'il intervienne a priori ou a posteriori, n'est pas exigé en tant que tel par la loi pour caractériser la loyauté de la collecte.

Compte-tenu de l'accessibilité universelle de l'internet, qui constitue une des principales caractéristiques et un des principaux atouts de ce réseau de communication mondial et décentralisé, un tel recueil -considéré en lui-mène et indépendamment de l'usage qui est ensuite fait des adresses collectées, qui n' est pas davantage un des éléments constitutifs de cette première infraction- de données disponibles sur des espaces publics, opération qui n'est interdite par aucune disposition expresse et n'implique l'usage d'aucun procédé frauduleux, ne peut être, du seul fait qu'il serait effectué sans que les intéressés en soient informés, considéré comme déloyal.

Il y a donc lieu d'entrer en voie de relaxe, du chef du délit de violation de l'interdiction établie par l'article 25 de la loi.

Le second délit institué par l' article 226-18 résulte de la violation des prescriptions de l'article 26 de la loi qui dispose que "toute personne physique est en droit de s'opposer, pour des raisons légitimes, à ce que des informations nominatives la concernant fassent l'objet d'un traitement". Il suppose donc, pour être constitué, le non-respect du droit d'opposition reconnu à toute personne physique à l'égard des données nominatives la concernant, dès lors que celles-ci font l'objet d'un fichier ou d'un traiterfient automatisé quelconque.

Il résulte de la procédure que, comme il a été relevé plus haut, à de très nombreuses reprises, les destinataires de messages adressés à la suite de l'utilisation, par leur expéditeur, des logiciels robotmail ou freeprospect n'ont pas été en mesure de faire valoir effectivement ce droit d'opposition, faute que le lien de désinscription offert à cet effet fonctionne effectivement.

Le tribunal n'est cependant pas saisi de ces faits, qui ne sont pas visés dans la citation, laquelle ne mentionne, ni pour l'un, ni pour l'autre des logiciels qu'elle incrimine, le non-respect de la faculté d'opposition -faculté qui ne peut concerner qu'un traitement déjà en cours-, mais vise une absence de consentement indubitable de la personne concernée qui n'est pas sanctionnée pénalement en l'état par les dispositions invoquées.

S'il n'est pas contesté, en effèt, que, dans le cadre des débats en cours sur une éventuelle réforme du droit applicable à la matière, notamment pour tenir compte des exigences d'une directive européenne du 12juillet 2002 relative à la protection des données personnelles dans le secteur des communications électroniques, les termes de l'alternative entre système de consentement préalable (dit "opt-in") ou mécanisme fondé sur le droit d'opposition ("opt-out") sont maintenant clairement définis, les règles pénales applicables à la présente espèce s'apparentent strictement à un simple droit d'opposition et excluent une quelconque exigence de consentement formel et préalable à tout traitement de donnée nominative, à laquelle se réfère à tort la prévention.

Dans ces conditions, sans qu'il soit besoin d'examiner les autres éléments constitutifs de cette seconde infraction, il y a lieu de renvoyer également le prévenu des fins de la poursuite de ce chef."

Note : J. LE CLAINCHE, *LES « POURRIELS » : LE DROIT DEPASSE PAR LA TECHNIQUE ?*, RLDI 2005/05, n° 141, p. 28.
Extrait de l'article

Référence : Tribunal de grande instance de Paris, 17ème Chambre, 07 décembre 2004, *MINISTÈRE PUBLIC C/ FABRICE H.*, DROIT-TIC
http://www.droit-tic.com/juris/aff.php?id_juris=2

TEXTES OFFICIELS

DIRECTIVE 2006/24/CE du Parlement européen et du Conseil du 15 mars 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

DIRECTIVE 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006

Directive 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

JOCE n° L 105 du 13 avr. 2006, , p. 54 à 63

LE PARLEMENT EUROPÉEN ET LE CONSEIL DE L'UNION EUROPÉENNE,

Vu le traité instituant la Communauté européenne, et notamment son article 95,

Vu la proposition de la Commission,

Vu l'avis du Comité économique et social européen (1),

Statuant conformément à la procédure visée à l'article 251 du traité (2),

considérant ce qui suit :

(1) La directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (3) oblige les États membres à assurer la protection des libertés et droits fondamentaux des personnes physiques, notamment de leur vie privée, à l'égard du traitement des données à caractère personnel, afin d'assurer la libre circulation de ces données dans la Communauté.

(2) La directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques) (4) traduit les principes définis dans la directive 95/46/CE en règles spécifiques au secteur des communications électroniques.

(3) Les articles 5, 6 et 9 de la directive 2002/58/CE définissent les règles applicables au traitement, par les fournisseurs de réseaux et de services, de données relatives au trafic et de données de localisation générées par l'utilisation de services de communications électroniques. Ces données doivent être effacées ou rendues anonymes lorsqu'elles ne sont plus nécessaires à la transmission d'une communication, sauf les données requises pour établir les factures et les paiements pour interconnexion; moyennant l'accord de l'intéressé,
certaines données peuvent également être traitées à des fins commerciales ou de fourniture de services à valeur ajoutée.

(4) L'article 15, paragraphe 1, de la directive 2002/58/CE énumère les conditions dans lesquelles les États membres peuvent limiter la portée des droits et des obligations prévus aux articles 5 et 6, à l'article 8, paragraphes 1, 2 , 3 et 4, et à l'article 9 de ladite directive. Toute limitation de ce type doit constituer une mesure nécessaire, appropriée et proportionnée, au sein d'une société démocratique, pour des raisons spécifiques d'ordre public, à savoir pour sauvegarder la sécurité nationale (c'est-à-dire la sûreté de l'État), la défense et la sécurité publique, ou pour assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales ou d'utilisations non autorisées de systèmes de communications électroniques.

(5) Plusieurs États membres ont légiféré sur la conservation de données par les fournisseurs de services en vue de la prévention, de la recherche, de la détection et de la poursuite d'infractions pénales. Lesdites dispositions nationales varient considérablement.

(6) Les disparités législatives et techniques existant entre les dispositions nationales relatives à la conservation de données en vue de la prévention, de la recherche, de la détection et de la poursuite d'infractions pénales constituent des entraves au marché intérieur des communications électroniques dans la mesure où les fournisseurs de services doivent satisfaire à des exigences différentes pour ce qui est des types de données relatives au trafic et à la localisation à conserver ainsi que des conditions et durées de conservation.

(7) Dans ses conclusions, le Conseil « Justice et affaires intérieures » du 19 décembre 2002 souligne qu'en raison de l'accroissement important des possibilités qu'offrent les communications électroniques, les données relatives à l'utilisation de celles-ci sont particulièrement importantes et constituent donc un instrument utile pour la prévention, la recherche, la détection et la poursuite d'infractions pénales, notamment de la criminalité organisée.

(8) Dans sa déclaration du 25 mars 2004 sur la lutte contre le terrorisme, le Conseil européen a chargé le Conseil d'envisager des propositions en vue de l'établissement de règles relatives à la conservation, par les fournisseurs de services, des données relatives au trafic des communications.

(9) En vertu de l'article 8 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales (CEDH), toute personne a droit au respect de sa vie privée et de sa correspondance. Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire, entre autres, à la sécurité nationale, à la sûreté publique, à la défense de l'ordre et à la prévention des infractions pénales, ou à la protection des droits et libertés d'autrui. Étant donné que la conservation des données s'est révélée être un outil d'investigation nécessaire et efficace pour les enquêtes menées par les services répressifs dans plusieurs États membres et, en particulier, relativement aux affaires graves telles que celles liées à la criminalité organisée et au terrorisme, il convient de veiller à ce que les données conservées soient accessibles aux services répressifs pendant un certain délai, dans les conditions prévues par la présente directive. L'adoption d'un instrument relatif à la conservation des données constitue dès lors une mesure nécessaire au regard des exigences de l'article 8 de la CEDH.

(10) Le 13 juillet 2005, le Conseil a réaffirmé, dans sa déclaration condamnant les attentats terroristes de Londres, la nécessité d'adopter dans les meilleurs délais des mesures communes relatives à la conservation de données concernant les télécommunications.

(11) Eu égard à l'importance des données relatives au trafic et des données de localisation pour la recherche, la détection et la poursuite d'infractions pénales, il est nécessaire, comme les travaux de recherche et l'expérience pratique de plusieurs États membres le démontrent, de garantir au niveau européen la conservation pendant un certain délai, dans les conditions prévues par la présente directive, des données traitées par les fournisseurs de communications électroniques dans le cadre de la fourniture de services de communications électroniques accessibles au public ou d'un réseau public de communications.

(12) L'article 15, paragraphe 1, de la directive 2002/58/CE continue à s'appliquer aux données, y compris celles relatives aux appels téléphoniques infructueux, dont la conservation n'est pas expressément requise par la présente directive et qui ne relèvent donc pas de son champ d'application, ainsi qu'à la conservation de données à d'autres fins que celles prévues par la présente directive, notamment à des fins judiciaires.

(13) La présente directive ne porte que sur les données générées ou traitées par suite d'une communication ou d'un service de communication et non sur le contenu proprement dit des informations communiquées. Les données devraient être conservées de manière à éviter qu'elles ne soient conservées plus d'une fois. Les données générées ou traitées, lors de la fourniture des services de communications concernés, concernent uniquement les données qui sont accessibles. En particulier, s'agissant de la conservation des données concernant le courrier électronique par l'Internet et la téléphonie par l'Internet, l'obligation de conserver les données peut ne s'appliquer qu'à l'égard des données émanant des propres services des opérateurs ou des fournisseurs de réseau.

(14) Les technologies liées aux communications électroniques progressent rapidement, et les exigences légitimes des autorités compétentes peuvent évoluer. Afin d'obtenir des avis et d'encourager la mise en commun des meilleures pratiques à ce sujet, la Commission a l'intention d'instituer un groupe composé des services répressifs des États membres, des associations du secteur des communications électroniques, de représentants du Parlement européen et des autorités chargées de la protection des données, y compris le contrôleur européen de la protection des données.

(15) La directive 95/46/CE et la directive 2002/58/CE sont pleinement applicables aux données conservées conformément à la présente directive. L'article 30, paragraphe 1, point c), de la directive 95/46/CE exige la consultation du groupe de travail sur la protection des personnes à l'égard du traitement des données à caractère personnel institué par l'article 29 de ladite directive.

(16) Les obligations incombant aux prestataires de services concernant les mesures visant à garantir la qualité des données, qui résultent de l'article 6 de la directive 95/46/CE, tout comme leurs obligations concernant les mesures visant à garantir la confidentialité et la sécurité du traitement des données, qui résultent des articles 16 et 17 de ladite directive, sont pleinement

applicables aux données qui sont conservées au sens de la présente directive.

(17) Il est fondamental que les États membres prennent des mesures législatives pour faire en sorte que les données conservées en vertu de la présente directive ne soient transmises qu'aux autorités nationales compétentes conformément à la législation nationale et dans le respect total des droits fondamentaux des personnes concernées.

(18) Dans ce contexte, l'article 24 de la directive 95/46/CE fait obligation aux États membres de sanctionner les violations des dispositions prises en application de ladite directive. L'article 15, paragraphe 2, de la directive 2002/58/CE impose la même obligation en ce qui concerne les dispositions nationales prises en application de la directive 2002/58/CE. La décision-cadre 2005/222/JAI du Conseil du 24 février 2005 relative aux attaques visant les systèmes d'information (5) prévoit que l'accès illicite intentionnel aux systèmes d'information, y compris aux données qui y sont conservées, est considéré comme une infraction pénale punissable.

(19) Le droit de toute personne ayant subi un dommage du fait d'un traitement illicite ou de toute autre action incompatible avec les dispositions nationales prises en application de la directive 95/46/CE d'obtenir réparation, qui découle de l'article 23 de ladite directive, s'applique également en cas de traitement illicite de toute donnée à caractère personnel au titre de la présente directive.

(20) La convention de 2001 du Conseil de l'Europe sur la cybercriminalité ainsi que la convention de 1981 du Conseil de l'Europe sur la protection des personnes à l'égard du traitement automatisé des données à caractère personnel s'appliquent également aux données conservées au sens de la présente directive.

(21) Étant donné que les objectifs de la présente directive, à savoir l'harmonisation des obligations incombant aux fournisseurs de conserver certaines données et de faire en sorte que ces données soient disponibles aux fins de la recherche, de la détection et de la poursuite d'infractions graves telles que définies par chaque État membre dans son droit interne, ne peuvent pas être réalisés de manière suffisante par les États membres et peuvent donc, en raison des dimensions ou des effets de la présente directive, être mieux réalisés au niveau communautaire, la Communauté peut prendre des mesures conformément au principe de subsidiarité consacré à l'article 5 du traité. Conformément au principe de proportionnalité, tel qu'énoncé audit article, la présente directive n'excède pas ce qui est nécessaire pour atteindre ces objectifs.

(22) La présente directive respecte les droits fondamentaux et observe les principes reconnus, notamment, par la Charte des droits fondamentaux de l'Union européenne. La présente directive ainsi que la directive 2002/58/CE visent notamment à veiller à ce que les droits fondamentaux liés au respect de la vie privée et des communications des citoyens et à la protection des données à caractère personnel, tels que consacrés aux articles 7 et 8 de la Charte, soient pleinement respectés.

(23) Étant donné que les obligations incombant aux fournisseurs de services de communications électroniques devraient être proportionnées, la présente directive leur prescrit de ne conserver que les données qui sont générées ou traitées lors de la fourniture de services de communication. Dans les cas où ces données ne sont pas générées ou traitées par ces fournisseurs, il n'y a pas d'obligation de les conserver. La présente directive n'a pas pour objectif d'harmoniser la technologie utilisée pour la conservation des données, le choix de celle-ci étant une question à régler au niveau national.

(24) Conformément au point 34 de l'accord interinstitutionnel « Mieux légiférer » (6), les États membres seront encouragés à établir, pour eux-mêmes et dans l'intérêt de la Communauté, leurs propres tableaux, qui illustrent, dans la mesure du possible, la concordance entre la présente directive et les mesures de transposition, et à les rendre publics.

(25) La présente directive est sans préjudice du pouvoir qu'ont les États membres d'adopter des mesures législatives concernant le droit pour les autorités nationales qu'ils ont désignées d'accéder aux données et de les utiliser. Les questions relatives à l'accès aux données conservées en application de la présente directive par les autorités nationales aux fins des activités visées à l'article 3, paragraphe 2, premier tiret, de la directive 95/46/CE ne relèvent pas du droit communautaire. Elles peuvent toutefois faire l'objet de dispositions de droit interne ou de mesures relevant du titre VI du traité sur l'Union européenne. De telles dispositions ou mesures doivent pleinement respecter les droits fondamentaux tels qu'ils découlent des traditions constitutionnelles communes des États membres et tels qu'ils sont consacrés par la CEDH. L'article 8 de la CEDH, tel qu'interprété par la Cour européenne des droits de l'homme, prévoit que toute ingérence d'une autorité publique dans l'exercice du droit au respect de la vie privée doit satisfaire aux exigences de nécessité et de proportionnalité et doit donc poursuivre des finalités déterminées, explicites et légitimes, et être exercée d'une façon qui soit appropriée, pertinente et non excessive au regard de l'objectif poursuivi,

ONT ARRÊTÉ LA PRÉSENTE DIRECTIVE :

Article premier
Objet et champ d'application

1. La présente directive a pour objectif d'harmoniser les dispositions des États membres relatives aux obligations des fournisseurs de services de communications électroniques accessibles au public ou de réseaux publics de communications en matière de conservation de certaines données qui sont générées ou traitées par ces fournisseurs, en vue de garantir la disponibilité de ces données à des fins de recherche, de détection et de poursuite d'infractions graves telles qu'elles sont définies par chaque État membre dans son droit interne.

2. La présente directive s'applique aux données relatives au trafic et aux données de localisation concernant tant les entités juridiques que les personnes physiques, ainsi qu'aux données connexes nécessaires pour identifier l'abonné ou l'utilisateur enregistré. Elle ne s'applique pas au contenu des communications électroniques, notamment aux informations consultées en utilisant un réseau de communications électroniques.

Article 2
Définitions

1. Aux fins de la présente directive, les définitions contenues dans la directive 95/46/CE, la directive 2002/21/CE du Parlement européen et du Conseil du 7 mars 2002 relative à un cadre réglementaire commun pour les réseaux et services de communications électroniques (directive « cadre ») (7), ainsi que dans la directive 2002/58/CE s'appliquent.

2. Aux fins de la présente directive, on entend par :

a) « données » les données relatives au trafic et les données de localisation, ainsi que les données connexes nécessaires pour identifier l'abonné ou l'utilisateur ;

b) « utilisateur » toute entité juridique ou personne physique qui utilise un service de communications électroniques accessible au public à des fins privées ou professionnelles sans être nécessairement abonnée à ce service ;

c) « service téléphonique » les appels téléphoniques (notamment les appels vocaux, la messagerie vocale, la téléconférence et la communication de données), les services supplémentaires (notamment le renvoi et le transfert d'appels), les services de messagerie et multimédias (notamment les services de messages brefs, les services de médias améliorés et les services multimédias) ;

d) « numéro d'identifiant » le numéro d'identification exclusif attribué aux personnes qui s'abonnent ou s'inscrivent à un service d'accès à l'Internet ou à un service de communication par l'Internet ;

e) « identifiant cellulaire » le numéro d'identification de la cellule où un appel de téléphonie mobile a commencé ou a pris fin ;

f) « appel téléphonique infructueux » toute communication au cours de laquelle un appel téléphonique a été transmis mais est resté sans réponse ou a fait l'objet d'une intervention de la part du gestionnaire du réseau.

Article 3
Obligation de conservation de données

1. Par dérogation aux articles 5, 6 et 9 de la directive 2002/58/CE, les États membres prennent les mesures nécessaires pour que les données visées à l'article 5 de la présente directive soient conservées, conformément aux dispositions de cette dernière, dans la mesure où elles sont générées ou traitées dans le cadre de la fourniture des services de communication concernés par des fournisseurs de services de communications électroniques accessibles au public ou d'un réseau public de communications, lorsque ces fournisseurs sont dans leur ressort.

2. L'obligation de conserver les données visées au paragraphe 1 inclut la conservation des données visées à l'article 5 relatives aux appels téléphoniques infructueux, lorsque ces données sont générées ou traitées, et stockées (en ce qui concerne les données de la téléphonie) ou journalisées (en ce qui concerne les données de l'Internet), dans le cadre de la fourniture des services de communication concernés, par des fournisseurs de services de communications électroniques accessibles au public ou d'un réseau public de communications, lorsque ces fournisseurs sont dans le ressort de l'État membre concerné. La présente directive n'impose pas la conservation des données relatives aux appels non connectés.

Article 4
Accès aux données

Les États membres prennent les mesures nécessaires pour veiller à ce que les données conservées conformément à la présente directive ne soient transmises qu'aux autorités nationales compétentes, dans des cas précis et conformément au droit interne. La procédure à suivre et les conditions à remplir pour avoir accès aux données conservées dans le respect des exigences de nécessité et de proportionnalité sont arrêtées par chaque État membre dans son droit interne, sous réserve des dispositions du droit de l'Union européenne ou du droit international public applicables en la matière, en particulier la CEDH telle qu'interprétée par la Cour européenne des droits de l'homme.

Article 5
Catégories de données à conserver

1. Les États membres veillent à ce que soient conservées en application de la présente directive les catégories de données suivantes :

a) les données nécessaires pour retrouver et identifier la source d'une communication :
1) en ce qui concerne la téléphonie fixe en réseau et la téléphonie mobile :
i) le numéro de téléphone de l'appelant ;
ii) les nom et adresse de l'abonné ou de l'utilisateur inscrit ;
2) en ce qui concerne l'accès à l'Internet, le courrier électronique par l'Internet et la téléphonie par l'Internet:
i) le(s) numéro(s) d'identifiant attribué(s) ;
ii) le numéro d'identifiant et le numéro de téléphone attribués à toute communication entrant dans le réseau téléphonique public ;
iii) les nom et adresse de l'abonné ou de l'utilisateur inscrit à qui une adresse IP (protocole Internet), un numéro d'identifiant ou un numéro de téléphone a été attribué au moment de la communication ;

b) les données nécessaires pour identifier la destination d'une communication :
1) en ce qui concerne la téléphonie fixe en réseau et la téléphonie mobile :
i) le(s) numéro(s) composé(s) [le(s) numéro(s) de téléphone appelé(s)] et, dans les cas faisant intervenir des services complémentaires tels que le renvoi ou le transfert d'appels, le(s) numéro(s) vers le(s)quel(s) l'appel est réacheminé ;
ii) les nom et adresse de l'abonné (des abonnés) ou de l'utilisateur (des utilisateurs) inscrit(s) ;
2) en ce qui concerne le courrier électronique par l'Internet et la téléphonie par l'Internet :
i) le numéro d'identifiant ou le numéro de téléphone du (des) destinataire(s) prévu(s) d'un appel téléphonique par l'Internet ;
ii) les nom et adresse de l'abonné (des abonnés) ou de l'utilisateur (des utilisateurs) inscrit(s) et le numéro d'identifiant du destinataire prévu de la communication ;

c) les données nécessaires pour déterminer la date, l'heure et la durée d'une communication :
1) en ce qui concerne la téléphonie fixe en réseau et la téléphonie mobile, la date et l'heure de début et de fin de la communication ;
2) en ce qui concerne l'accès à l'Internet, le courrier électronique par l'Internet et la téléphonie par l'Internet :
i) la date et l'heure de l'ouverture et de la fermeture de la session du service d'accès à l'Internet dans un fuseau horaire déterminé, ainsi que l'adresse IP (protocole Internet), qu'elle soit dynamique ou statique, attribuée à une communication par le fournisseur d'accès à l'Internet, ainsi que le numéro d'identifiant de l'abonné ou de l'utilisateur inscrit ;
ii) la date et l'heure de l'ouverture et de la fermeture de la session du service de courrier électronique par l'Internet ou de téléphonie par l'Internet dans un fuseau horaire déterminé ;

d) les données nécessaires pour déterminer le type de communication :
1) en ce qui concerne la téléphonie fixe en réseau et la téléphonie mobile, le service téléphonique utilisé ;
2) en ce qui concerne le courrier électronique par l'Internet et la téléphonie par l'Internet, le service Internet utilisé ;

e) les données nécessaires pour identifier le matériel de communication des utilisateurs ou ce qui est censé être leur matériel :
1) en ce qui concerne la téléphonie fixe en réseau, le numéro de téléphone de l'appelant et le numéro appelé ;
2) en ce qui concerne la téléphonie mobile :
i) le numéro de téléphone de l'appelant et le numéro appelé ;
ii) l'identité internationale d'abonné mobile (IMSI) de l'appelant ;
iii) l'identité internationale d'équipement mobile (IMEI) de l'appelant ;
iv) l'IMSI de l'appelé ;
v) l'IMEI de l'appelé ;
vi) dans le cas des services anonymes à prépaiement, la date et l'heure de la première activation du service ainsi que l'identité de localisation (identifiant cellulaire) d'où le service a été activé ;
3) en ce qui concerne l'accès à l'Internet, le courrier électronique par l'Internet et la téléphonie par l'Internet :
i) le numéro de téléphone de l'appelant pour l'accès commuté ;
ii) la ligne d'abonné numérique (DSL) ou tout autre point terminal de l'auteur de la communication ;

f) les données nécessaires pour localiser le matériel de communication mobile :
1) l'identité de localisation (identifiant cellulaire) au début de la communication ;
2) les données permettant d'établir la localisation géographique des cellules, en se référant à leur identité de localisation (identifiant cellulaire), pendant la période au cours de laquelle les données de communication sont conservées.

2. Aucune donnée révélant le contenu de la communication ne peut être conservée au titre de la présente directive.

Article 6
Durées de conservation

Les États membres veillent à ce que les catégories de données visées à l'article 5 soient conservées pour une durée minimale de six mois et maximale de deux ans à compter de la date de la communication.

Article 7
Protection et sécurité des données

Sans préjudice des dispositions adoptées en application des directives 95/46/CE et 2002/58/CE, chaque État membre veille à ce que les fournisseurs de services de communications électroniques accessibles au public ou d'un réseau public de communications respectent, au minimum, les principes suivants en matière de sécurité des données, pour ce qui concerne les données conservées conformément à la présente directive :

a) les données conservées doivent être de la même qualité et soumises aux mêmes exigences de sécurité et de protection que les données sur le réseau ;

b) les données font l'objet de mesures techniques et organisationnelles appropriées afin de les protéger contre la destruction accidentelle ou illicite, la perte ou l'altération accidentelle, ou le stockage, le traitement, l'accès ou la divulgation non autorisés ou illicites ;

c) les données font l'objet de mesures techniques et organisationnelles appropriées afin de garantir que l'accès aux données n'est effectué que par un personnel spécifiquement autorisé, et

d) les données sont détruites lorsque leur durée de conservation prend fin, à l'exception des données auxquelles l'on a pu accéder et qui ont été préservées.

Article 8
Conditions à observer pour le stockage des données conservées

Les États membres veillent à ce que les données visées à l'article 5 soient conservées conformément à la présente directive de manière ce que les données conservées et toute autre information nécessaire concernant ces données puissent, à leur demande, être transmises sans délai aux autorités compétentes.

Article 9
Autorité de contrôle

1. Chaque État membre désigne une ou plusieurs autorités publiques qui sont chargées de surveiller l'application, sur son territoire, des dispositions adoptées par les États membres en application de l'article 7 pour ce qui concerne la sécurité des données conservées. Ces autorités peuvent être les mêmes que celles visées à l'article 28 de la directive 95/46/CE.

2. Les autorités visées au paragraphe 1 exercent en toute indépendance la surveillance visée audit paragraphe.

Article 10
Statistiques

1. Les États membres font en sorte que des statistiques sur la conservation de données traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public soient transmises annuellement à la Commission. Ces statistiques comprennent notamment :

- les cas dans lesquels des informations ont été transmises aux autorités compétentes conformément à la législation nationale applicable,
- le laps de temps écoulé entre la date à partir de laquelle les données ont été conservées et la date à laquelle les autorités compétentes ont demandé leur transmission,
- les cas dans lesquels des demandes de données n'ont pu être satisfaites.

2. Ces statistiques ne contiennent pas de données à caractère personnel.

Article 11
Modification de la directive 2002/58/CE

À l'article 15 de la directive 2002/58/CE, le paragraphe suivant est inséré :
« 1 bis. Le paragraphe 1 n'est pas applicable aux données dont la conservation est spécifiquement exigée par la directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006 sur la conservation de données traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communication (8) aux fins visées à l'article 1er, paragraphe 1, de ladite directive.

Article 12
Mesures ultérieures

1. Un État membre confronté à des circonstances particulières justifiant une prolongation, pour une période limitée, de la durée de conservation maximale prévue à l'article 6, peut prendre les mesures nécessaires. L'État membre notifie immédiatement à la Commission et communique aux autres États membres les mesures prises en vertu du présent article et les motive.

2. Dans un délai de six mois suivant la notification visée au paragraphe 1, la Commission approuve ou rejette les

mesures nationales concernées après avoir vérifié si elles représentent ou non un moyen de discrimination arbitraire ou une restriction déguisée aux échanges entre États membres, et si elles constituent ou non une entrave au fonctionnement du marché intérieur. En l'absence de décision de la Commission dans ce délai, les mesures nationales sont réputées approuvées.

3. Lorsque, en application du paragraphe 2, les mesures nationales d'un État membre dérogeant aux dispositions de la présente directive sont approuvées, la Commission peut examiner s'il y a lieu de proposer une adaptation de la présente directive.

Article 13
Recours, responsabilité et sanctions

1. Chaque État membre prend les mesures nécessaires pour veiller à ce que les mesures nationales mettant en œuvre le chapitre III de la directive 95/46/CE relatif aux recours juridictionnels, à la responsabilité et aux sanctions, soient intégralement appliquées au traitement des données effectué au titre de la présente directive.

2. Chaque État membre prend, en particulier, les mesures nécessaires pour faire en sorte que l'accès intentionnel aux données conservées conformément à la présente directive ou le transfert de ces données qui ne sont pas autorisés par le droit interne adopté en application de la présente directive, soient passibles de sanctions, y compris de sanctions administratives ou pénales, qui sont efficaces, proportionnées et dissuasives.

Article 14
Évaluation

1. Le 15 septembre 2010 au plus tard, la Commission présente au Parlement européen et au Conseil une évaluation de l'application de la présente directive et de ses effets sur les opérateurs économiques et les consommateurs, compte tenu de l'évolution de la technologie des communications électroniques et des statistiques transmises à la Commission en vertu de l'article 10 afin de déterminer s'il y a lieu de modifier les dispositions de la présente directive, notamment la liste des données prévue à l'article 5 et les durées de conservation prévues à l'article 6. Les conclusions de cette évaluation sont rendues publiques.

2. À cette fin, la Commission examine toute observation qui pourrait lui être transmise par les États membres ou le groupe de travail institué par l'article 29 de la directive 95/46/CE.

Article 15
Transposition

1. Les États membres mettent en vigueur les dispositions législatives, réglementaires et administratives nécessaires pour se conformer à la présente directive le 15 septembre 2007 au plus tard. Ils en informent immédiatement la Commission. Lorsque les États membres adoptent ces dispositions, celles-ci contiennent une référence à la présente directive ou sont accompagnées d'une telle référence lors de leur publication officielle. Les modalités de cette référence sont arrêtées par les États membres.

2. Les États membres communiquent à la Commission le texte des dispositions essentielles de droit interne qu'ils adoptent dans le domaine régi par la présente directive.

3. Chaque État membre peut, jusqu'au 15 mars 2009, différer l'application de la présente directive en ce qui concerne la conservation de données de communication concernant l'accès à l'Internet, la téléphonie par l'Internet et le courrier électronique par l'Internet. Tout État membre qui a l'intention de recourir au présent paragraphe le notifie au Conseil et à la Commission au moyen d'une déclaration lors de l'adoption de la présente directive. La déclaration est publiée au *Journal officiel de l'Union européenne*.

Article 16
Entrée en vigueur

La présente directive entre en vigueur le vingtième jour suivant celui de sa publication au *Journal officiel de l'Union européenne*.

Article 17
Destinataires

Les États membres sont destinataires de la présente directive.

Fait à Strasbourg, le 15 mars 2006.

Par le Parlement européen
Le président, J. Borrell Fontelles

Par le Conseil
Le président, H. Winkler

(1) Avis émis le 19 janvier 2006 (non encore paru au Journal officiel)
(2) Avis du Parlement européen du 14 décembre 2005 (non encore paru au Journal officiel) et décision du Conseil du 21 février 2006.
(3) JO L 281 du 23.11.1995, p. 31. Directive modifiée par le règlement (CE) n° 1882/2003 (JO L 284 du 31.10.2003, p. 1).

(4) JO L 201 du 31.7.2002, p. 37.
(5) JO L 69 du 16.3.2005, p. 67.
(6) JO C 321 du 31.12.2003, p. 1.
(7) JO L 108 du 24.4.2002, p. 33.
(8) JO L 105 du 13.4.2006, p. 54.

Déclaration des Pays-Bas au titre de l'article 15, paragraphe 3, de la directive 2006/24/CE

En ce qui concerne la directive du Parlement européen et du Conseil sur la conservation de données traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public, et modifiant la directive 2002/58/CE, les Pays-Bas recourent à la possibilité de différer l'application de la directive à la conservation de données de communication concernant l'accès à l'internet, la téléphonie par l'internet et le courrier électronique par l'internet pendant une période de dix-huit mois au plus à compter de la date d'entrée en vigueur de la directive.

Déclaration de l'Autriche au titre de l'article 15, paragraphe 3, de la directive 2006/24/CE

L'Autriche déclare qu'elle différera, pour une période de dix-huit mois à compter de la date visée à l'article 15, paragraphe 1, l'application de la présente directive à la conservation de données de communication concernant l'accès à l'internet, la téléphonie par l'internet et le courrier électronique par l'internet.

Déclaration de l'Estonie au titre de l'article 15, paragraphe 3, de la directive 2006/24/CE

Conformément à l'article 15, paragraphe 3, de la directive du Parlement européen et du Conseil 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, l'Estonie fait part de son intention de recourir audit paragraphe et de différer l'application de cette directive en ce qui concerne la conservation de données de communication concernant l'accès à l'internet, la téléphonie par l'internet et le courrier électronique par l'internet pendant une période de trente-six mois à compter de la date d'adoption de ladite directive.

Déclaration du Royaume-Uni au titre de l'article 15, paragraphe 3, de la directive 2006/24/CE

Le Royaume-Uni déclare, conformément à l'article 15, paragraphe 3, de la directive 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, qu'il différera l'application de ladite directive à la conservation de données de communication concernant l'accès à l'internet, la téléphonie par l'internet et le courrier électronique par l'internet.

Déclaration de Chypre au titre de l'article 15, paragraphe 3, de la directive 2006/24/CE

Chypre déclare qu'elle différera l'application de la présente directive en ce qui concerne la conservation de données de communication concernant l'accès à l'internet, ainsi que les services de courrier électronique et de téléphonie par l'internet jusqu'à la date visée à l'article 15, paragraphe 3.

Déclaration de la Grèce au titre de l'article 15, paragraphe 3, de la directive 2006/24/CE

La Grèce déclare qu'elle différera, conformément à l'article 15, paragraphe 3, l'application de la présente directive en ce qui concerne la conservation de données de communication concernant l'accès à l'internet, ainsi que les services de courrier électronique et de téléphonie par l'internet pour une période maximale de dix-huit mois à compter de l'expiration du délai prévu à l'article 15, paragraphe 1.

Déclaration du Luxembourg au titre de l'article 15, paragraphe 3, de la directive 2006/24/CE

Conformément à l'article 15, paragraphe 3, de la directive du Parlement européen et du Conseil 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, le gouvernement du Grand-Duché de Luxembourg déclare qu'il entend recourir audit article 15, paragraphe 3, de la directive afin d'avoir la possibilité de différer l'application de cette directive en ce qui concerne la conservation de données de communication concernant l'accès à l'internet, la téléphonie par l'internet et le courrier électronique par l'internet.

Déclaration de la Slovénie au titre de l'article 15, paragraphe 3, de la directive 2006/24/CE

La Slovénie se joint au groupe des États membres ayant fait une déclaration en vertu de l'article 15, paragraphe 3, de la directive du Parlement européen et du Conseil 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, en vue d'un report de dix-huit mois de l'application de ladite directive à la conservation de données de communication concernant l'accès à l'internet, la téléphonie par l'internet et le courrier électronique par l'internet.

Déclaration de la Suède au titre de l'article 15, paragraphe 3, de la directive 2006/24/CE

La Suède entend, conformément à l'article 15, paragraphe 3, avoir la possibilité de différer l'application de la directive en ce qui concerne la conservation de données de communication concernant l'accès à l'internet, la téléphonie par l'internet et le courrier électronique par l'internet.

Déclaration de la Lituanie au titre de l'article 15, paragraphe 3, de la directive 2006/24/CE

Conformément à l'article 15, paragraphe 3, de la proposition de directive du Parlement européen et du Conseil 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 communication, et modifiant la directive 2002/58/CE (ci-après dénommée «la directive»), la Lituanie déclare que, lorsque la directive aura été adoptée, elle différera son application à la conservation de données de communication concernant l'accès à l'internet, la téléphonie par l'internet et le courrier électronique par l'internet, comme prévu à l'article 15, paragraphe 3.

Déclaration de la Lettonie au titre de l'article 15, paragraphe 3, de la directive 2006/24/CE

Conformément à l'article 15, paragraphe 3, de la directive 2006/24/CE 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, la Lettonie déclare qu'elle diffère l'application de cette directive en ce qui concerne la conservation de données de communication concernant l'accès à l'internet, la téléphonie par l'internet et le courrier électronique par l'internet jusqu'au 15 mars 2009.

Déclaration de la République tchèque au titre de l'article 15, paragraphe 3, de la directive 2006/24/CE

Conformément à l'article 15, paragraphe 3, de la directive susmentionnée, la République tchèque déclare qu'elle diffère l'application de cette directive en ce qui concerne la conservation de données de communication concernant l'accès à l'internet, la téléphonie par l'internet et le courrier électronique par l'internet pendant une période de trente-six mois à compter de la date de son adoption.

Déclaration de la Belgique au titre de l'article 15, paragraphe 3, de la directive 2006/24/CE

La Belgique déclare différer, conformément à la possibilité prévue à l'article 15, paragraphe 3, et pour une période de trente-six mois après l'adoption de la présente directive, son application en ce qui concerne la conservation des données de communication concernant l'accès à l'internet, la téléphonie par l'internet et le courrier électronique par l'internet.

Déclaration de la Pologne au titre de l'article 15, paragraphe 3, de la directive 2006/24/CE

La Pologne déclare qu'elle recourt à la possibilité prévue à l'article 15, paragraphe 3, de la directive du Parlement européen et du Conseil 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, qui lui permet de différer l'application de ladite directive à la conservation de données de communication concernant l'accès à l'internet, la téléphonie par l'internet et le courrier électronique par l'internet pendant une période de dix-huit mois à compter de la date visée à l'article 15, paragraphe 1.

Déclaration de la Finlande au titre de l'article 15, paragraphe 3, de la directive 2006/24/CE

La Finlande déclare, conformément à l'article 15, paragraphe 3, de la directive 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, qu'elle différera l'application de ladite directive à la conservation de données de communication concernant l'accès à l'internet, la téléphonie par l'internet et le courrier électronique par l'internet.

Déclaration de l'Allemagne au titre de l'article 15, paragraphe 3, de la directive 2006/24/CE

L'Allemagne se réserve le droit de différer, pendant une période de dix-huit mois à compter de la date visée à l'article 15, paragraphe 1, l'application de la directive à la conservation de données de communication concernant l'accès à l'internet, la téléphonie par l'internet et le courrier électronique par l'internet.

DROIT-TIC .com

R.D.T.I.C

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

ARTICLE 29 Data Protection Working Party

Opinion n° 3/2006, 25 mar. 2006, relative à la directive 2006/24/CE sur la conservation des données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou des réseaux publics de communication et modifiant la directive n° 2002/58/CE, WP 119, 654/06/EN

This Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC.

THE WORKING PARTY ON THE PROTECTION OF INDIVIDUALSWITH REGARD TO THE PROCESSING OF PERSONAL DATA

Set up by Directive 95/46/EC of the European Parliament and of the Council of 24 October 19951,
having regard to Articles 29 and 30 (1)(a) and (3) of that Directive and 15(3) of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002,
having regard to its Rules of Procedure, and in particular Articles 12 and 14 thereof,

has adopted the following Opinion:

On 21 February 2006 the Council adopted Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks services and amending Directive 2002/58/EC2. The European Parliament had approved the Commission proposal (COM (2005) 0438)3 as amended during the negotiations with the Council and accordingly adopted a legislative resolution on 14 December 2005 (C6-0293/2005 – 2005/0182(COD)).

In its last Opinion WP 113 of 21 October 2005 on the then draft Directive, the Art. 29 Working Party had voiced its reservations since the provisions of the Directive will have far reaching consequences for all European citizens and their privacy. The decision to retain communication data for the purpose of combating serious crime is an unprecedented one with a historical dimension. It encroaches into the daily life of every citizen and may endanger the fundamental values and freedoms all European citizens enjoy and cherish. The Working Party recalls the considerations and concerns set out in the aforementioned Opinion which retain their validity. It is, therefore, of utmost importance that the Directive is accompanied and implemented in each Member State by measures curtailing the impact on privacy.

The Art. 29 Working Party notes that the Directive lacks some adequate and specific safeguards as to the treatment of communication data and leaves room for diverging interpretation and implementation by the Member States in this respect. However, adequate and specific safeguards are necessary to protect the vital interests of the individual as mentioned by Directive 2002/58/EC, in particular the right to confidentiality when using publicly available electronic communications services. The Working Party considers it also crucial that the provisions of the Directive are interpreted and implemented in a harmonised way to ensure that the European citizens can enjoy throughout the European Union the same level of protection.

Therefore, the Art. 29 Working Party proposes a uniform, European-wide implementation of the Directive. This approach should guarantee a harmonized application of the provisions of the Directive whilst respecting the highest level possible of protecting personal data. This should also be done with a view to reducing the considerable costs to be borne by the service providers when complying with the provisions of the Directive.

In order to transpose the provisions of the Directive in a uniform way and to comply with the requirements of Article 8 of the European Convention on Human Rights, Member States should implement adequate and specific safeguards. At least the following safeguards should be taken into account:

1)Purpose specification: The data should only be retained for specific purposes. Therefore, the term "serious crime" should be clearly defined and delineated. Any further processing should be ruled out or limited stringently on the basis of specific safeguards.
2)Access limitation: The data should only be available to specifically designated law enforcement authorities where necessary for the investigation, detection, and prosecution of the offences referred to in the Directive. A list of such designated law enforcement authorities should be made public. Any retrieval of the data should be recorded and the records made available to the supervisory authority/ies in order to ensure an effective supervision.

3)Data minimisation: The data to be retained should be kept to a minimum, and any changes to that list should be subject to a strict necessity test.
4)No data mining: Investigation, detection and prosecution of the offences referred to in the Directive should not entail large-scale data-mining based on retained data, in respect of the travel and communication patterns of people unsuspected by law enforcement authorities.

5)Judicial/ independent scrutiny of authorized access: Access to data should, in principle, be duly authorised on a case by case basis by judicial authorities without prejudice to countries where a specific possibility of access is authorised by law, subject to independent oversight. Where appropriate, the authorisations should specify the particular data required for the specific case at hand.

6)Retention purposes of providers: Providers of public electronic communication services or networks are not allowed to process data retained solely for public order purposes under the Data Retention Directive for other purposes, especially their own.

7)System separation: In particular, the systems for storage of data for public order purposes should be logically separated from the systems used for business purposes.

8)Security measures: Minimum standards should be defined concerning the technical and organisational security measures to be taken by providers, specifying more in detail the general requirements of the Directive on data retention.

The Art. 29 Working Party calls on the Member States to co-ordinate the implementation of the data retention Directive into national laws in order to guarantee a harmonised approach across the European Union and to uphold the high standard of data protection provided by both Directives 1995/46/EC and 2002/58/EC.
Done at Brussels, on 25 March 2006
For the Working Party

1. OJ L 281, 23.11.1995, p. 31, http://europa.eu.int/comm/justice_home/fsj/privacy/law/index_en.htm.

2. OJ L 105, 13.04.2006, p.54.

3. OJ C 49, 28.2.2006, p. 42.