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

ANALYSES

FOCUS

TEXTES OFFICIELS

JURISPRUDENCE

DOCTRINE DE LA CNIL

DROIT-TIC .com

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

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

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

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

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

Vous pouvez présenter vos observations, remarques, 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

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

SOMMAIRE

FOCUS

ANALYSES

ACTUALITÉ

TEXTES OFFICIELS

JURISPRUDENCES

DOCTRINE DE LA CNIL

NOMS DE DOMAINE, PROPRIÉTÉS INDUSTRIELLES ET COMMERCIALES

COUR DE CASSATION, CHAMBRE CRIMINELLE, 6 SEPTEMBRE 2005 : PAS DE PROTECTION PÉNALE DU NOM DE DOMAINE

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

Le nom de domaine non enregistré ne peut, en droit français, bénéficier de la protection de la marque

Pour soutenir la campagne d'un candidat à la présidence de Madagascar, un informaticien avait depuis la France développé un site web. Ce site, accessible à l'adresse tiako-i-madagasikara.com, retraçait jour après jour les événements de la vie politique malgache, et consistait en articles, photos, forums, etc. Le fonctionnement du site prenait beaucoup de temps à son développeur. Afin que le site soit nourri en son absence, le développeur en confia « les clefs » à un tiers (communication de la totalité des codes d'accès et du contenu des sources permettant de modifier ou restaurer la base de données). Après avoir été évincé de la campagne présidentielle, il se retrouve aussi privé de site : son (ex) homme de confiance l'a fermé, et a réservé le nom de domaine tiako-i-madagasikara.org, pour y publier... l'intégralité des données figurant à l'origine sur le site qu'il a fermé. Le créateur le cite en justice.

Le demandeur est débouté de son action pénale en contrefaçon de marque par la Cour d'appel de Versailles (18 novembre 2004), qui a naturellement relevé qu'une action en défense d'un nom de domaine ne peut être fondée sur le fondement pénal de l'article L. 716-9 du Code de la propriété intellectuelle. Il n'obtient pas non plus la condamnation pénale du défendeur pour atteinte aux droits sur sa base de données, la Cour ayant considéré que le producteur d'une base ne peut reprocher l'extraction du contenu de sa base s'il n'a pas préalablement interdit une telle extraction (et la cour infirme le jugement qui avait aussi retenu l'infraction de maintien frauduleux dans un système de traitement automatisé (T.corr. Nanterre, 25 mars 2003)). Pourvoi est formé.

Il est soutenu que le nom de domaine est un signe susceptible de représentation graphique qui servait en l'espèce à distinguer des services, et qu'à ce titre il a les caractéristiques d'une marque, partant la protection de l'article L. 716-9. Il est en outre soutenu que la cour d'appel a ajouté à la loi en conditionnant l'application de la protection du producteur à la formulation d'une interdiction préalable.

La Cour de cassation rejette le pourvoi, et approuve l'arrêt d'appel dans les termes suivants :

"*Attendu que les énonciations de l'arrêt attaqué mettent la Cour de cassation en mesure de s'assurer que la cour d'appel a, sans insuffisance ni contradiction, et en répondant aux chefs péremptoires des conclusions dont elle était saisie, exposé les motifs pour lesquels elle a estimé que la preuve des infractions reprochées n'était pas rapportée à la charge du prévenu, en l'état des éléments soumis à son examen, et a ainsi justifié sa décision déboutant la partie civile de ses prétentions ;*
D'où il suit que les moyens, qui, pour le second est inopérant en ce qu'il allègue une violation de l'article 323-1 du Code pénal non visé à la prévention, et qui se bornent, pour le surplus, à remettre en question l'appréciation souveraine, par les juges du fond, des faits et circonstances de la cause, ainsi que des éléments de

preuve contradictoirement débattus, ne sauraient être admis"

Il est donc confirmé - si besoin était - que le nom de domaine non enregistré ne peut, en droit français, bénéficier de la protection de la marque. Cet arrêt de la Cour de cassation, non publié, n'a donc pas vocation à rester dans les annales (ce qui est heureux au regard de l'autre question posée, relative à la base de données : sur ce point, le pourvoi est rejeté pour raisons procédurales).

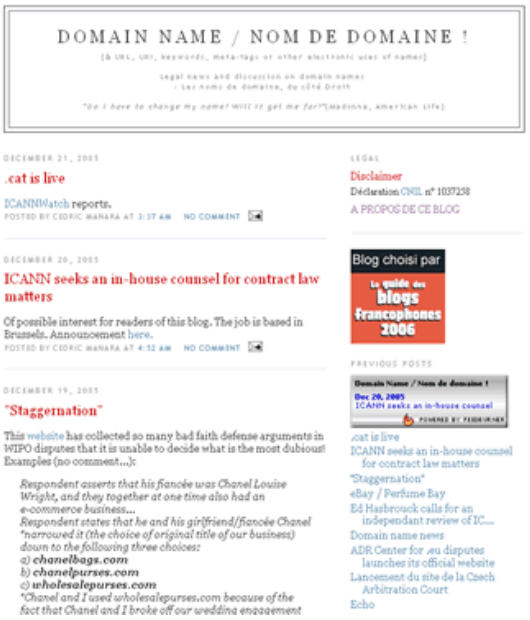
Cour de Cassation, Ch. Crim., arrêt du 26 septembre 2005, ROJO R. C/ GUY R. <http://www.droit-tic.com/juris/aff.php?id_juris=56>.

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

Domaine Name / Nom de domaine

[& URL, URI, keywords, meta-tags or other electronic uses of names]
Legal news and discussion on domain names - Les noms de domaine, du côté Droit

"*Do I have to change my name? Will it get me far?*"(Madonna, American Life)



<http://domaine.blogspot.com>

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

C. Cass., Ch. Crim., arrêt du 26 septembre 2005, ROJO R. C/ GUY R

Thèmes
Adressage, Noms de domaine et liens hypertextes, Propriétés industrielles et commerciales

Abstract
Noms de domaine, charte nommage, reproduction d'une marque (oui), protection par le droit des marques (oui), base de données, interdiction préalable de l'extraction (non), investissement financier, matériel ou humain substantiel (oui), protection (oui)

Résumé
Un nom de domaine ne peut jouir d'une protection par le droit des marques que s'il reproduit celle-ci ou une dénomination très proche prêtant à confusion. La protection d'un base de données ne nécessite pas l'interdiction de l'extraction.

Décision

Cour de Cassation
Chambre criminelle
Audience publique du 6 septembre 2005 | Rejet
N° de pourvoi : 04-87303
Inédit

Président : M. COTTE

REPUBLIQUE FRANCAISE
AU NOM DU PEUPLE FRANCAIS
AU NOM DU PEUPLE FRANCAIS
LA COUR DE CASSATION, CHAMBRE CRIMINELLE, en son audience publique tenue au Palais de Justice à PARIS, le six septembre deux mille cinq, a rendu l'arrêt suivant :

Sur le rapport de M. le conseiller LE CORROLLER, les observations de Me SPINOSI, de la société civile professionnelle TIFFREAU, avocats en la Cour, et les conclusions de M. l'avocat général CHEMITHE ;
Statuant sur le pourvoi formé par :

- X... Rojo, partie civile,

contre l'arrêt de la cour d'appel de VERSAILLES, 9ème chambre, en date du 18 novembre 2004[1], qui l'a débouté de ses demandes après relaxe de Guy <NO >RANDRIANARISONY... des chefs de contrefaçon de marque et atteinte aux droits du producteur d'une base de données ;

Vu les mémoires produits en demande et en défense ;
Sur le premier moyen de cassation, pris de la violation des articles, L. 711-1, L. 713-1, L. 716-1, L. 716-9 du Code de la propriété intellectuelle, 591 et 593 du Code de procédure pénale ;

"en ce que l'arrêt attaqué a infirmé le jugement ayant déclaré Guy Y... coupable de contrefaçon de marques ;

"aux motifs qu'un nom de domaine Internet permet de situer une machine sur le réseau en utilisant des lettres plutôt que des chiffres, comme c'est le cas pour les numéros de téléphone, et ce, afin de faciliter sa mémorisation et son utilisation ; chaque nom de domaine est associé à une " adresse IP " qui est une sorte de code de l'emplacement de la machine hébergeant le site sur l'Internet ; l'administration de chaque extension locale est confiée à une structure dépendant du pays de l'extension ; ces organismes sont la plupart du temps appelés " NIC ", abréviation de " Network Information Center " ;

ainsi, en France, c'est l'Association française pour le Nommage Internet en Coopération (AFNIC) qui est le gestionnaire de la base de données des noms de domaine géographiques .fr (France) et .re (île de la Réunion) ; les suffixes génériques (.com, .net, .org) sont gérés par la société de droit américain Network Solutions ; les règles fixées par les NIC compétente doivent être respectées pour enregistrer un nom de domaine ; ces règles constituent une " charte de nommage " qui est, selon les pays, plus ou moins ouverte (autorisant les dépôts sans justificatifs ou exigeant des justificatifs et des conditions précises) ; il résulte de ce qui précède que la notion de nom de domaine, spécifique au monde de l'Internet, est totalement distincte de celle de marque ; une marque est, en effet, un signe distinctif pouvant être apposé sur un produit ou accompagnant une prestation de service et destiné à informer le public sur sa provenance industrielle ou commerciale ; elle fait l'objet d'une procédure d'enregistrement effectuée à la demande de la personne qui en réclame l'appropriation ; en France, cet enregistrement se fait auprès de l'Institut national de la propriété industrielle (INPI), et pour les marques communautaires, il se fait auprès de l'Office d'harmonisation dans les marchés intérieurs (OHMI) basé à Alicante, en Espagne ; au niveau mondial, l'organisme compétent est l'organisation mondiale de la propriété intellectuelle (OMPI) ; aux termes de l'article L. 713-1 du Code de la propriété intellectuelle, "

[1] http://www.legalis.net/breves-article.php3?id_article=1387

l'enregistrement confère à son titulaire un droit de propriété sur cette marque pour les produits et les services qu'il a désignés " ; la protection que confèrent les dispositions pénales de l'article L. 716-9 du Code de la propriété intellectuelle ne s'applique qu'aux marques enregistrées ; n'en bénéficient que les propriétaires tels que définis plus haut ; cette protection ne pourrait s'appliquer à un nom de domaine Internet que si celui-ci reproduisait la dénomination d'une marque déposée ou d'une dénomination très proche prêtant à confusion ; en l'espèce, le nom de domaine dont se prévaut la partie civile, d'une part, ne possède aucune caractéristique d'une marque et, d'autre part, n'a fait l'objet d'aucun enregistrement qui conférerait à Rojo X... un droit de propriété au sens de l'article L. 713-1 du Code de la propriété intellectuelle ; il se déduit de ce qui précède que la prévention de contrefaçon de marque n'est aucunement établie dans cette affaire ;

la Cour, en conséquence, relaxera Guy Y... des fins de la poursuite " ;

"alors que le signe susceptible de représentation graphique " http://www.tiako-i-madagasikara.com " permettant de distinguer les services offerts par la partie civile dans le cadre de la campagne des élections présidentielles malgaches, le nom de domaine " http://www.tiako-i-madagasikara.com " possédait donc bien, contrairement à ce qu'a retenu la cour d'appel, les caractéristiques d'une marque ; que l'enregistrement du nom de domaine a conféré à la partie civile un droit de propriété sur cette marque qui devait bénéficier de la protection conférée par les dispositions pénales de l'article L. 716-9 du Code de la propriété intellectuelle" ;

Sur le second moyen de cassation, pris de la violation des articles L. 341-1, L. 342-1, L. 342-2 du Code de la propriété intellectuelle, 591 et 593 du Code de procédure pénale ;

"en ce que l'arrêt attaqué a infirmé le jugement ayant déclaré Guy Y... coupable d'atteinte à la protection sur les bases de données ;

"aux motifs qu'il convient au préalable d'indiquer que la référence à " l'article L. 341-1 et suivants de la loi n° 98-536 du 1er juillet 1998 " est erronée ; la Cour considérera que la partie civile vise en réalité l'incrimination prévue par l'article L. 343-1 du Code de la propriété intellectuelle, qui vise les atteintes aux droits définis à l'article L. 341-1 du même code, ces dispositions ayant été introduites dans le Code de la propriété intellectuelle par la loi 98-536 du 1er juillet 1998 ; les articles L. 341-1, L. 342-1, L. 342-2 et L. 343-1 du Code de la propriété intellectuelle (insérés dans ce code par la loi n° 98-536 du 1er juillet 1998) disposent :

article L. 341-1 : " le producteur d'une base de données, entendu comme la personne qui prend l'initiative et le risque des investissements correspondants, bénéficie d'une protection du contenu de la base lorsque la constitution, la vérification ou la présentation de celui-ci atteste d'un investissement financier, matériel ou humain substantiel ; cette protection est indépendante et s'exerce sans préjudice de celles résultant du droit d'auteur ou d'un autre droit sur la base de données ou un de ses éléments constitutifs " ; article L. 342-1 : " le producteur de bases de données a le droit d'interdire : 1) l'extraction, par transfert permanent ou temporaire de la totalité ou d'une partie qualitativement ou quantitativement substantielle du contenu d'une base de données sur un autre support, par tout moyen et sous toute forme que ce soit ; 2) la réutilisation, par la mise à la disposition du public de la totalité ou d'une partie qualitativement ou quantitativement substantielle du contenu de la base, quelle qu'en soit la forme ; ces droits peuvent être transmis ou cédés ou faire l'objet d'une licence ; le prêt public n'est pas un acte d'extraction ou de réutilisation " ; article L. 342-2 : " le producteur peut également interdire l'extraction ou la réutilisation répétée et systématique de parties qualitativement ou quantitativement non substantielles du contenu de la base lorsque ces opérations excèdent manifestement les conditions d'utilisation normale de la base de données " ; article L. 343-1 dans sa rédaction en vigueur au moment des faits (rédaction résultant de la loi du 1er juillet 1998, la loi du 9 mars 2004 n'ayant pas modifié l'incrimination mais aggravé les peines et ajouté la circonstance aggravante éventuelle de bande organisée) : " est puni de deux ans d'emprisonnement et de 1 000 000 francs (150 000 euros) d'amende le fait de porter atteinte aux droits du producteur d'une base de données tels que définis à l'article L. 342-1 " ; il se déduit de ce qui précède que l'incrimination insérée par la loi du 1er juillet 1998 dans le Code de la propriété intellectuelle vise l'atteinte portée au droit reconnu au producteur de base de données par l'article L. 342-1 précité ; ce droit consiste en la possibilité reconnue au producteur d'une base de données d'interdire qu'il soit procédé par autrui à l'extraction par transfert du contenu de ladite base de données sur un autre support ou par la réutilisation par la mise à la disposition du public de la totalité ou d'une partie qualitativement ou quantitativement substantielle du contenu de la base, quelle qu'en soit la forme ;

l'incrimination pénale visée par la citation directe de Rojo X... suppose donc que le producteur qui se dit lésé ait préalablement interdit l'extraction du contenu de sa base de données, faute de quoi cette dernière ne disposera pas de la protection instaurée par la disposition pénale citée plus haut ; il n'est, en l'espèce, aucunement allégué par la partie civile qu'une telle interdiction ait été émise par Rojo X... ; l'infraction pénale visée par la poursuite, même à supposer établis les faits dénoncés par la partie civile, n'est en conséquence pas constituée, faute d'élément légal " ;

"alors que la protection instaurée par la loi du 1er juillet 1998 est accordée au producteur dès lors que

la constitution, la vérification ou la présentation du contenu de la base atteste d'un investissement financier, matériel ou humain substantiel ; qu'en considérant que cette protection suppose que le producteur qui se dit lésé ait préalablement interdit l'extraction du contenu de sa base de données, la cour d'appel a ajouté à la loi une condition qu'elle ne comporte pas ; qu'en l'espèce, la base de données produite par la partie civile bénéficiant, même si celle-ci n'avait pas émis d'interdiction expresse et préalable, de la protection instaurée par l'article L. 341-1 du Code de la propriété intellectuelle, l'élément légal de l'infraction de modification de données résultant du maintien frauduleux dans un système de traitement automatisé, visée par la prévention, était, contrairement à ce qu'a retenu la cour d'appel, constitué" ;

Les moyens étant réunis ;
Attendu que les énonciations de l'arrêt attaqué mettent la Cour de cassation en mesure de s'assurer que la cour d'appel a, sans insuffisance ni contradiction, et en répondant aux chefs péremptoires des conclusions dont elle était saisie, exposé les motifs pour lesquels elle a estimé que la preuve des infractions reprochées n'était pas rapportée à la charge du prévenu, en l'état des éléments soumis à son examen, et a ainsi justifié sa décision déboutant la partie civile de ses prétentions ;
D'où il suit que les moyens, qui, pour le second est inopérant en ce qu'il allègue une violation de l'article 323-1 du Code pénal non visé à la prévention, et qui se bornent, pour le surplus, à remettre en question l'appréciation souveraine, par les juges du fond, des faits et circonstances de la cause, ainsi que des éléments de preuve contradictoirement débattus, ne sauraient être admis ;

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, dans la formation prévue à l'article L.131-6, alinéa 4, du Code de l'organisation judiciaire : M. Cotte président, M. Le Corroller conseiller rapporteur, M. Blondet conseiller de la chambre ;
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 ;

L'arrêt sur Legifrance.
<http://www.legifrance.gouv.fr/WAspad/UnDocument?base=INCA&nod=IXRXCX2005X09X06X00873X003>

Référence : Cour de Cassation, Ch. Crim., arrêt du 6 septembre 2005, *ROJO R. C/ GUY R.*, DROIT-TIC
http://www.droit-tic.com/juris/aff.php?id_juris=56

NOMS DE DOMAINE, ADMINISTRATION ÉLECTRONIQUE

LE .EU BOUDÉ PAR LES GRANDES VILLES FRANCAISES

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

Sur les 10 principales villes françaises, seules trois d'entre elles sont en mesure d'obtenir leurs .eu.

Sur les 10 principales villes françaises, seules trois d'entre elles sont en mesure d'obtenir leurs .eu, et quatre n'ont pas fait l'objet de demandes de noms de domaine en .eu. Découvrez comment l'appel du ministre de l'Industrie pour la protection des collectivités locales n'a pas été entendu par tous.

François Loos, avait pourtant attiré l'attention des entreprises et des organismes français sur le début de la « sunrise period » pour le .eu. Six villes et pas des moindres (la capitale parisienne, Marseille, Lyon, Toulouse, Bordeaux et Rennes) n'ont pas soumis la moindre demande d'enregistrement à l'Eurid*.

Un podium abandonné

Pour certaines, il est encore temps. La cité phocéenne (2ième ville de France, en termes de population), Lyon (3ième), Toulouse (4ième) et Rennes (10ième) peuvent encore soumettre leurs demandes à leur « registrar » (bureau officiel d'enregistrement) et être premiers !

Un astucieux hollandais

Pour Paris, Nice, et Bordeaux, il faudra passer devant une même société basée aux Pays-Bas, nommée Traffic Web Holding BV. Cette entreprise a fait valoir des droits antérieurs sur la base de marque nationale enregistrée, respectivement : Par&is, n&ice, et bord&eaux. En effet, pour les marques enregistrées comprenant une esperluette, cette dernière peut être remplacée par un -, et ou and, mais aussi tout simplement retiré... Dommage pour la ville de Nice (3ième dans la file d'attente), mais la demande hollandaise pourrait bien être validée par l'agent de validation PricewaterhouseCoopers Belgique (PWC).

Madré, Traffic Web Holding a utilisé le même procédé pour être premier sur london.eu, avec comme marque revendiquée lon&don. En tout cas, elle n'aura pas madrid.eu ou berlin.eu.

L'Espagne et l'Allemagne avaient pris le soin de protéger le nom de leurs capitales (lire notre précedent article), ceux qui n'ait pas le cas de la France, qui n'a pas protégé ses communes en .eu.

Retenons, tout de même les bons élèves nantais, strasbourgeois et montpelliérains en première position pour obtenir leurs villes en .eu. Comme quoi, l'appel du ministre n'était pas totalement vain !

* Cette étude a été réalisée le jeudi 8 décembre, à 10 heures, via le whois de l'Eurid, disponible sur www.whois.eu.

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

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 DE LA PREUVE, SIGNATURE ÉLECTRONIQUE

RECOMMANDATION DE LA CNIL SUR L'ARCHIVAGE ÉLECTRONIQUE DES DONNÉES PERSONNELLES DANS LES ENTREPRISES DU SECTEUR PRIVÉ

Par M. Vincent DOMNESQUE, Juriste TIC - BRM Avocat

Dans sa délibération n° 2005-213 du 11 octobre 2005, la CNIL a adopté une recommandation concernant les modalités d'archivage électronique, dans le secteur privé, de données à caractère personnel.

Dans sa délibération n° 2005-213 du 11 octobre 2005, la CNIL a adopté une recommandation concernant les modalités d'archivage électronique, dans le secteur privé, de données à caractère personnel.

Face au développement exponentiel de l'archivage électronique dans les entreprises, la Commission nationale de l'informatique et des libertés a rendu le 11 octobre 2005 une recommandation « visant à sensibiliser les professionnels sur certaines règles générales de bonnes pratiques à mettre en œuvre ».

La Commission relève qu'en vertu des dispositions légales, il incombe aux entreprises d'archiver pour des durées plus ou moins importantes, toutes les informations relevant de leur activité et concernant aussi bien les données comptables que fiscales ou les données sociales. Bien souvent ces données sont régies par les principes du droit à l'oubli ou de finalité consacrés par les articles 6-5° et 24 de la loi du 6 janvier 1978, modifiée par la loi du 6 août 2004, relative aux fichiers, à l'informatique et aux libertés. La Commission a entendu préciser les modalités de cet archivage électronique.

Tout d'abord, s'agissant de la durée de conservation des données, la CNIL souhaite que le responsable du traitement procède à la mise en place de procédures d'archivage distinctes suivant « les catégories de données » collectées. À cette fin, la Commission distingue trois catégories de données. En premier lieu, les données d'utilisation courantes qui peuvent être par exemple pour la CNIL « les données concernant un client dans le cadre de l'exécution d'un contrat ». En second lieu, les données intermédiaires « qui présentent encore pour les services concernés un intérêt administratif et dont les durées de conservation sont fixées par les règles de prescription applicables», par exemple en cas de contentieux. Enfin les données définitives « présentant un intérêt historique, scientifique ou statistique justifiant qu'elles ne fassent l'objet d'aucune destruction ». En outre le responsable doit être en mesure d'effectuer, le cas échéant, « toute purge ou destruction sélective de données ».

Sur la sécurité des données archivées, la Commission recommande s'agissant des archives intermédiaires ou des archives définitives que leur accès soit limité à « un service spécifique » de l'entreprise, comme par exemple le service des archives de l'entreprise lorsqu'il s'agit d'archives définitives. Également, l'accès aux archives définitives ne devrait être possible que par un « accès distinct, ponctuel et précisément motivé auprès de ce service spécifique seul habilité à consulter ce type d'archives ». De surcroît, la Commission indique la nécessité pour l'entreprise de « garantir l'intégrité des données archivées » ainsi que la mise en place de dispositifs permettant la « traçabilité des consultations des données archivées ».

En outre, la CNIL recommande, s'agissant des données sensibles relevant de l'article 8 de la loi « Informatique et

Libertés », des procédés d'anonymisation.

Enfin, la CNIL souhaite que les entreprises définissent, dans le cadre de « procédures formalisées », des règles d'archivage répondant à l'ensemble de ses préconisations. Ces règles pouvant être accessibles sur simple demande, à toutes personnes objet du traitement des données nominatives.

Par M. Vincent DOMNESQUE, Juriste TIC - BRM Avocat

BRM AVOCATS NEWS

Pour approfondir, consultez :

C.N.I.L, délibération N° 2005-213 du 11 octobre 2005, PORTANT ADOPTION D'UNE RECOMMANDATION CONCERNANT LES MODALITÉS D'ARCHIVAGE ÉLECTRONIQUE, DANS LE SECTEUR PRIVÉ, DE DONNÉES À CARACTÈRE PERSONNEL,

RDTIC, n° 47, nov. 2005, p. 39.

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 TRAVAIE

CORRESPONDANT INFORMATIQUE ET LIBERTÉS : UN ENCADREMENT JURIDIQUE INCOMPLET?

Par M. Cédric Crépin, Etudiant à l'IEJ d'Anger

Le dispositif, inscrit aux articles 22 et 67 de la loi « Informatique et Libertés » est désormais effectif grâce à la publication du décret du 20 octobre 2005

La Commission Nationale de l'Informatique et des Libertés (CNIL) a fêté en cette année 2005 son 25ème anniversaire. La longévité de l'institution de la rue Saint-Guillaume démontre l'importance que revêt le bras exécutif de la loi du 6 janvier 1978. Cependant, un malaise insidieux grandit depuis plusieurs années : la loi Informatique et Libertés, figure de proue du respect de la vie privée face à l'informatique et aux dangers qu'elle peut engendrer, n'est que peu appliquée. En ce sens, alors que tout traitement mettant en jeu des données personnelles doit être déclaré, il est regrettable de constater que de nombreuses entreprises et administrations agissent dans la clandestinité. Les causes sont multiples : complexité de la loi, voire ignorance pure et simple du texte, difficulté dans la mise en œuvre, crainte de dévoiler des données stratégiques… À cet état s'ajoute un manque de pragmatisme de la loi et de la CNIL face aux évolutions technologiques. La loi du 6 août 2004, transposition de la directive 95/46 CE, entend remettre « Informatique et Libertés » en phase avec les problèmes contemporains, mais aussi anticiper l'avenir. Car c'est là que le bât blesse : l'informatique et les méthodes de traitements évoluent vite, et il est nécessaire d'avoir un outil adapté afin de pouvoir réguler les trafics d'information. Cet outil, le législateur le trouve au sein de la directive 95/46 CE, plus précisément au considérant 18, qui dispose que les Etats ont la possibilité de recourir au système du « *détaché à la protection des données à caractère personnel chargé notamment d'assurer, d'une manière indépendante, l'application interne des dispositions nationales prises en application de la présente directive, et de tenir un registre des traitements effectués par le responsable de traitement […] garantissant de la sorte que les traitements ne sont pas susceptibles de porter atteinte aux droits et libertés des personnes concernées* ».

La motivation du législateur français en saisissant cette option laissée par le texte communautaire est de passer d'un système déclaratoire centralisé à un système d'exemption déconcentré, situé sur le terrain, au plus proche des responsables de traitements. Le dispositif, inscrit aux articles 22 et 67 de la loi « Informatique et Libertés » est désormais effectif grâce à la publication du décret du 20 octobre 2005 pour être mis en pratique. Après avoir attendu 10 ans pour transposer la directive 95/46 CE « Protection des données », ce qui fait de la France le dernier Etat de L'Union a avoir transposé ce texte, le législateur aura mis plus de 15 mois pour publier ce décret auquel on ne croyait plus. On peut s'interroger sur cette lenteur administrative, alors que la réadaptation du droit français aux problématiques informatiques devenait urgente, et surtout lorsqu'on se souvient que la France avait fait pression auprès de ses partenaires européens pour que soit adoptée la directive « Protection des données ».

Le Titre III du décret d'application de la loi du 6 août 2004 est entièrement consacré au correspondant à la protection des données à caractère personnel, ou selon la terminologie employée par la CNIL, correspondant informatique et libertés (CIL). Longtemps attendu, ce

texte doit fournir les indices nécessaires à l'encadrement et la mise en pratique de la fonction. Le CIL est désigné par le responsable de traitement, ce qui ouvre le dispositif aux administrations comme aux entreprises. Il peut être une personne physique ou morale, interne ou externe même si des restrictions demeurent. L'externalisation n'est pas autorisée « *lorsque plus de cinquante personnes sont chargées de la mise en oeuvre ou ont directement accès aux traitements ou catégories de traitements automatisés pour lesquels le responsable entend désigner un correspondant à la protection des données à caractère personnel* » (art. 42). Des exceptions sont toutefois ouvertes pour les groupes de sociétés, les GIE ou les organismes professionnels qui peuvent désigner un CIL travaillant en leur sein. Son rôle est de dresser une liste des traitements dont il a la charge, ce qui emporte une dispense de déclaration auprès de la CNIL de ces traitements. Ce « Monsieur Informatique et Libertés » a aussi pour rôle de conseiller le responsable lorsque de nouveaux traitements sont mis en œuvre, voire de l'alerter lorsqu'un risque de dérive existe. Véritable acteur de terrain, le CIL est le maillon appelé à réconcilier responsables de traitements et CNIL afin de mieux faire respecter les exigences légales, dont les infractions sont lourdement sanctionnées. Du côté de la CNIL, on espère une diminution des contraintes administratives et une pédagogie responsabilisante auprès des entreprises et administrations. Pour l'organisme désignant, ce peut être un moyen de s'épargner des tracasseries administratives, le tout en soignant une image de marque et en se conformant aux exigences légales. Cependant, à la lecture des textes, il est possible de discerner un certain vide dans l'encadrement. Une large marge de manœuvre est laissée à la pratique, mais on peut également regretter que certains points ne soient pas évoqués avec plus de précision.

La place de la CNIL

Si une grande marche de manœuvre est laissée aux responsables, il serait faux de croire que tout est permis. Faire du CIL une niche à exonération conduirait les organismes malveillants à des sanctions. Si aucun contrôle *a priori* n'est exercé par la CNIL, on peut imaginer que des contrôles « préventifs » seront organisés ou que des plaintes soient déposées envers un organisme ayant fait le choix du CIL, ce qui conduira inévitablement à un examen des procédés de l'organisme incriminé. La CNIL possède même un pouvoir de décharge du CIL lorsque des manquements graves sont constatés. Reste à déterminer le seuil de gravité qui sera retenu par la CNIL.

Mais pour ce « ménage à trois » entre le responsable de traitements, le CIL et la CNIL soit viable, encore faut-il que la CNIL dispose de moyens nécessaires à l'organisation et l'animation d'un réseau. La procédure ne désignation n'a d'autre intérêt que d'officialiser les rapports entre le CIL et la CNIL et d'établir le point de départ de la dispense accordée à l'organisme désignant. On peut alors s'interroger sur l'exhaustivité des renseignements demandés qui ne présentent que peu d'intérêt pour la CNIL. En revanche, ces données pourraient se révéler importantes pour l'information des tiers. Il est à souhaiter qu'à l'instar des autorités de contrôles hollandaises et luxembourgeoises, la CNIL tienne une liste des organismes ayant fait le choix d'un CIL, ce qui permettrait aux individus de saisir directement le CIL. Mais deux obstacles freinent cette idée : d'une part, c'est exposer le CIL à des prospections commerciales, et d'autre part, la CNIL doit obtenir l'accord des CIL personne physique pour pouvoir diffuser leur nom et coordonnées par respect du principe de l'"*opt-in*". Si la désignation autorise la CNIL à connaître l'ensemble des CIL désignés, saura-t-elle pour autant garder la main sur ceux-ci ? La création d'un maillage d'interlocuteurs réguliers est un des objectifs de la Commission qui envisage de fournir un traitement privilégié pour les CIL, via des interlocuteurs uniques, et qui s'illustrerait par la tenue de réunions régulières visant à la définition de standards professionnels, la recherche en commun de solutions aux problèmes vécus au quotidien par les CIL, etc. Si l'intention est louable, force est de constater que les moyens manquent. A l'heure actuelle, la « cellule CIL » n'est composée que d'un agent à temps plein. Si de nombreux CIL sont désignés, difficile d'imaginer qu'une seule personne puisse prendre en charge l'animation d'un réseau exigeant des moyens

financiers, logistiques et techniques relativement important. En Suède et aux Pays-Bas, de tels réseaux existent et rencontrent de francs succès, les initiatives étant nombreuses (newsletters, extranet, formations et séminaires…). Ces autorités bénéficient néanmoins de moyens relativement importants, alors qu'en France la CNIL est aux aboies, la promesse d'une enveloppe budgétaire étant renvoyée aux calanques grecques.

La formation

La désignation d'un CIL est une question d'opportunité pour les organismes. La France n'a pas voulu le rendre obligatoire, à l'inverse de l'Allemagne où les *Datenschutzbeaufragter* (DSB) existent depuis près de 30 ans, afin de laisser s'affirmer un esprit d'ouverture et de sensibilisation aux questions touchant à la protection des données à caractère personnel. Le mot d'ordre semble donc être « souplesse » : peuvent désigner un CIL ceux qui le veulent, selon le modèle de leur choix. Reste à déterminer qui peut être nommé à ce poste. Une double condition est ici posée. En premier lieu, le CIL ne doit pas exercer de fonction pouvant entraîner un conflit d'intérêt, ce qui élimine le responsable de traitement à la candidature, et doit en second lieu bénéficier « *des qualifications professionnelles requises pour exercer ses missions* » (Art. 22 L. 6 janvier 1978), le décret n'étayant pas cette disposition. Compétent en droit, en informatique, en management, beaucoup de compétences sont réclamées à un seul individu, ce qui peut favoriser l'essor des prestataires externes capables de mobiliser divers spécialistes. Pourtant, si les textes ne dresse pas les diplômes requis à l'exercice de la fonction, c'est une nouvelle forme de souplesse. La CNIL, lorsqu'elle recevra la notification de désignation, ne procédera pas à un contrôle d'opportunité. En somme, quelque soit la personne désignée, l'important est qu'elle soit compétente dans l'exercice des missions qui lui sont confiées. C'est donc au responsable de traitement d'établir au moment du recrutement la liste des qualifications requises, comme pour tout autre employé ou prestataire. Et il est facile de croire que des formations verront le jour afin d'approfondir les compétences les CIL en place.

Les relations contractuelles

Alors que le CIL prestataire est lié par un contrat de prestations de services à durée limitée, comment positionner la fonction du CIL lorsqu'il est salarié de l'organisme ? Faut-il amender le contrat de travail, rédiger un nouveau contrat ? Un parallèle avec les mandats sociaux peut être envisagé. Le CIL étant une fonction, elle fait l'objet d'un contrat de travail lorsqu'elle est occupée à plein temps. Par contre, si elle ne nécessite qu'une occupation à temps partiel, elle peut faire l'objet d'un mandat du même type que celui dont bénéficient les délégués du personnel. Emportant suspension du contrat de travail lorsqu'elle la personne effectue ses missions de CIL, le mandat permet d'exercer la fonction sans voir le contrat de travail rompu. Ainsi, lorsqu'il se verrait démettre de sa fonction, il pourrait retrouver son emploi habituel. Néanmoins, pour assurer une indépendance, il semble nécessaire de limiter dans le temps ce mandat. Qu'ils soient politiques ou sociaux, nombre d'entre eux sont à durée limitée ce qui assure une indépendance et un renouvellement nécessaire pour apporter un point de vue toujours plus neutre, sur les questions de protection de la vie privée en l'occurrence.

L'indépendance

L'un des dispositions les plus discutées de l'art. 22 III de la loi du 6 janvier 1978 concerne le statut du CIL. Il est prévu qu'il exerce ses missions de « *manière indépendante* », ne pouvant « *faire l'objet d'aucune sanction de la part de l'employeur du fait de l'accomplissement de ses missions* ». Le décret précise même en son art. 46 que « *Le correspondant ne reçoit aucune instruction pour l'exercice de sa mission* ». Alors même qu'il n'est pas un salarié protégé, le CIL est-il dès lors un électron libre au sein de l'organisme, ne souffrant aucune hiérarchie ? Cette disposition dont la rédaction est contestable mérite d'être éclairée. L'art. 46 du décret

porte en effet sur deux points essentiels :

* le CIL dispose d'un contact direct avec le responsable, c'est-à-dire qu'il doit pouvoir directement s'adresser à lui pour formuler toute recommandation ou demande, sans avoir à passer par une hiérarchie, ce qui le place à n'en pas douter à un poste haut placé dans l'organigramme de l'organisme ;

* le CIL ne peut exercer une autre fonction pouvant générer un conflit d'intérêt. Le décret fournit comme exemple le responsable de traitements, ce qui est somme toute logique puisqu'on ne peut être juge et partie. A cette incompatibilité de principe seront sans doute adjointes d'autres impossibilité, révélées par la pratique. La question du DRH ou du DSI, qui ont un pouvoir sur certains traitements, devra vite trouver une réponse.

Replacé dans ce contexte, l'indépendance doit semble t'il être analysée comme une indépendance d'esprit, c'est-à-dire la faculté de formuler les critiques et les recommandations nécessaires à une mise en conformité du traitement, en soulignant certains aspects négatifs, les services défaillants. Autrement dit, dans le cadre de ses missions, le CIL doit avoir la capacité de résister à la pression et l'influence, quelque soit la forme sous laquelle elle se manifeste. Néanmoins, tous les CIL auront-ils cette force de caractère de s'opposer voire de « dénoncer » auprès de la CNIL ceux qui les emploient ? La problématique est ici la même que celle à laquelle les commissaires aux comptes sont confrontés : se taire et risquer alors une faute dans l'exercice des missions, ou dénoncer les agissements illégaux au risque de perdre son emploi ou son client. De plus, l'une des sanctions envisageables envers un responsable ne respectant pas les obligations légales est un retour au système de déclaration. Qu'advient-il alors du CIL qui perd par l'annulation d'exemption sa principale tâche auprès de l'organisme l'employant ? La question prend tout son sens lorsque la prestation est externalisée puisque le contrat liant le CIL à l'organisme devient nécessairement caduc dans une telle hypothèse. Le risque pour le CIL est aussi de voir son image salie par une réputation d'incompétence. Il y a tout lieu de s'interroger sur la pertinence du dispositif qui se trouve biaisé par ses propres dispositions.

La responsabilité

La délégation de pouvoir

L'un des avantages escompté par les responsables par le biais du CIL est un transfert de responsabilité pénale. Ni la loi ni le décret ne prévoient de dispositions en la matière, ce qui ne signifie pas qu'elle est impossible. La délégation de pouvoirs est un moyen consacré par la jurisprudence pour permettre à un chef d'entreprise de s'exonérer de sa responsabilité pénale. En transférant à l'un des salariés une partie de ses fonctions, le dirigeant délègue aussi sa responsabilité pénale. Cinq arrêts de la Chambre criminelle de la Cour de cassation en date du 11 mars 1993 sont venus définir le régime actuel de la délégation de pouvoirs : « *Hors les cas où la loi en dispose autrement, le chef d'entreprise qui n'a pas personnellement pris part à la réalisation de l'infraction peut s'exonérer de sa responsabilité pénale s'il rapporte la preuve qu'il a délégué ses pouvoirs à une personne pourvue de la compétence, de l'autorité et des moyens nécessaires* ». En sa qualité de responsable de traitement, par défaut le chef d'entreprise, l'exonération de la responsabilité pénale est possible par la démonstration d'une absence de participation aux faits susceptibles d'être sanctionnés au titre des articles 131-13 et 226-16 à -22 du Code pénal, dont les infractions sont sanctionnées de peines supérieures à celles infligée en matière d'homicide involontaire.

* La participation aux faits : ces infractions pèsent sur le responsable de traitement. Il est la seule personne habilitée à intervenir lorsqu'il a connaissance des agissements du subordonné. La désignation d'un CIL n'emporte pas le transfert de cette obligation de surveillance et de contrôle de l'activité des salariés. De plus, c'est le responsable de traitement qui détermine les finalités et les moyens du traitement.

* La compétence : le CIL devant avoir les qualités

requises à l'exercice des missions qui lui sont confiées, il semble que cette exigence soit remplie

* Les moyens : La fonction de CIL exige une indépendance dans l'exercice des missions confiées. Pour assurer cette indépendance, le projet de décret précise que le responsable de traitement doit fournir au correspondant tout élément lui permettant d'établir et d'actualiser régulièrement une liste de traitements automatisés et doit prendre toute mesure utile en vue de l'accomplissement par le CIL de ses missions en matière de protection des données. A l'allocation de moyens est donc attachée une finalité. Or, dans le contexte d'une délégation de pouvoirs, ces moyens ne semblent pas pertinents pour assurer une responsabilité sur les traitements mis en œuvre, ce qui fait échec à l'exercice d'une délégation de pouvoirs.

* L'autorité : La notion d'autorité dans le cadre d'une délégation de pouvoirs est définie en jurisprudence comme le pouvoir de donner des instructions à un service. Or l'art. 22 III de la loi du 6 janvier 1978 dispose que le correspondant a pour mission d'assurer « *le respect des obligations prévues* » par la loi Informatique et Libertés, le décret précisant que le CIL n'a qu'une capacité d'alerte et de conseil, afin que le responsable de traitement puisse donner des directives aux services chargés des traitements de données. La fonction de CIL semble donc incompatible avec l'exercice d'une autorité quant à la mise en œuvre des traitements automatisés. Dès lors, l'absence d'autorité prive la fonction de CIL d'une des caractéristiques de la délégation de pouvoirs.

Le CIL ne semble donc pouvoir être destinataire d'une délégation de pouvoirs, ne cumulant pas l'ensemble des conditions nécessaires à son établissement. Cela va dans le sens du texte de la loi Informatique et Libertés qui, dans son esprit, ne veut pas faire du CIL un miroir aux alouettes, en l'entourant de garanties d'indépendance, sans en faire un salarié protégé. C'est aussi la direction prise par la jurisprudence qui, en posant strictement les conditions d'existence d'une délégation de pouvoirs, vise à les limiter et à instaurer une équité : à la quête de pouvoirs se conjugue l'exercice de responsabilités. Pour autant, le CIL n'est pas un « intouchable » aux yeux de la justice. Si lui transférer des responsabilités qui ne sont en définitive pas les siennes est impossible, le correspondant peut parfaitement engager sa responsabilité propre en certaines circonstances.

La complicité

On peut ainsi envisager le cas où le responsable de traitement violerait les obligations posées par la loi Informatique et Libertés, et ce avec le CIL qui pourrait aider à la commission de l'infraction, par action (en effectuant un acte matériel) ou par omission (le CIL sait qu'une infraction est commise mais ne la signale pas). Dans ce cas de figure, il est nécessaire d'envisager que le CIL a la conscience et la volonté d'aider à la commission de l'infraction. Toutes les conditions seraient alors réunies pour poursuivre le CIL au titre de la complicité punie par l'art. 121-6 du Code pénal.

La négligence

Conseil et non pas contrôleur, que se passe-t-il lorsque le CIL constate une irrégularité mais ne formule aucune recommandation afin de corriger cette défaillance ? Autrement dit, alors que le responsable de traitement, sous le couvert de la bonne foi, commet une irrégularité, le CIL, en ayant pris conscience ne la signale pas. Ce n'est plus ici la complicité qui s'applique, car la faute du responsable, si elle est commise sous l'empire de la négligence ou de l'omission, n'est pas constitutive d'une infraction. Le silence du CIL peut-il être ici coupable ? Là encore, ni la loi ni le projet de décret ne prévoient de dispositions spécifiques sur ces questions, et il reviendra alors à la jurisprudence de trancher. Deux situations sont envisageables. D'une part, le CIL s'abstient de révéler les faits en temps utiles. La non révélation peut alors être analysée comme un délit d'abstention, distinct de la complicité. D'autre part, le CIL manifeste l'intention de ne pas révéler les faits qui est ici coupable, sous couvert de prouver la connaissance des faits délictueux, car elle constitue la preuve de la volonté de commettre un délit.

L'art. 22 III de la loi du 6 janvier 1978 met à la charge du

CIL la tenue d'une liste des traitements dispensés de déclarations. Que se passe-t-il si cette liste n'est pas tenue, ou de façon incomplète ? Le non accomplissement des formalités déclaratives est lourdement puni. Cependant aucune sanction n'est spécialement prévue en cas de liste incomplète. Ce paradoxe doit-il amener à penser que par parallélisme, la faute portant sur les formalités déclaratives vaut aussi pour la liste dont le CIL a la charge ? Ou doit-on y voir un oubli du législateur ? La loi pénale étant d'interprétation stricte, il est impossible d'assimiler la liste comme l'équivalent des formalités déclaratoires, et donc de sanctionner tout défaut dans sa tenue par l'art. 226-16 du Code pénal, punissant de 5 ans d'emprisonnement et de 300 000 euros d'amendes les fautes dans l'établissement des formalités déclaratives. Un argument important en faveur de la désignation d'un CIL...

Par M. Cédric Crépin, Etudiant à l'IEJ d'Anger

Pour approfondir, consultez :

C. CREPIN, LE CORRESPONDANT INFORMATIQUE ET LIBERTÉS, UN NOUVEL OUTIL DE RÉGULATION POUR LA PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL,

DROIT-TIC, Oct. 2005.

DROIT-TIC .com

R.D.T.I.C

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

JURISPRUDENCES

CA Paris, 4ème Chambre Section A, arrêt du 22 juin 2005, FRANKLIN L. ET SOCIÉTÉ SMILEY WORLD LTD. C/ SNC AOL BERTELSMAN ON LINE

Thèmes
Propriétés industrielles et commerciales, responsabilité

Abstract
Propriété industrielle, marque figurative, nullité de la marque (non), dégénérescence de la marque (non), contrefaçon (oui), concurrence déloyale et parasitaire (oui).

Résumé
En reproduisant et diffusant sur son site Internet l'icône représentant un visage souriant, illustrant le texte « Je suis content », la société AOL FRANCE a commis des actes de contrefaçon par imitation des marques N° 1 695 775 et N° 97 668 059...

Décision

« RÉPUBLIQUE FRANCAISE

AU NOM DU PEUPLE FRANCAIS

COUR D'APPEL DE PARIS

4e Chambre – Section A

ARRÊT DU 22 JUIN 2005

Numéro d'inscription au répertoire général : 04/09761

Décision déférée à la Cour : Jugement du 02 Mars 2004 –Tribunal de Grande Instance de CRÉTEIL – RU n° 02/4616

APPELANTS

Monsieur Franklin L.
représenté par la SCP MOREAU Jean et Alain, avoués à la Cour
assisté de Me Damien RÉGNIER, avocat au barreau de Paris, toque : D451

STE SMILEYWORLD LIMITED
ayant son siège 21 Bruton Street
LONDRES WIX 8DJ Royaume-Uni
prise en la personne de ses représentants légaux
représentée par la SCP MOREAU JEAN ET ALAIN, avoués à la Cour
assistée de Me Damien RÉGNIER, avocat au barreau de Paris, toque : D451

INTIMÉE

S.N.C. AOL BERTELSMAN ON LIGNE
ayant son siège immeuble FRANCE 118/123 avenue Charles de Gaulle 92200 NEUILLY SUR SEINE
prise en la personne de ses représentants légaux
représentée par la SCP ROBLIN – CHAIX DE LAVARENE, avoués à la Cour
assistée de Me Étienne WÉRY, avocat au barreau de Paris, toque P098, plaidant pour la SCP ULYS

COMPOSITION DE LA COUR

L'affaire a été débattue le 24 Mai 2005, en audience publique, devant la Cour composée de :
Monsieur Alain CARRE-PIERRAT, Président
Madame Marie-Gabrielle MAGUEUR, Conseiller
Madame Dominique ROSENTHAL-ROLLAND, Conseiller
qui en ont délibéré

Greffier, lors des débats : Mme Jacqueline VIGNAL

ARRÊT

- prononcé publiquement par Monsieur Alain CARRE-PIERRAT, Président.
- signé par Monsieur Alain CARRE-PIERRAT, président et par Mme Jacqueline VIGNAL, greffier, à laquelle la minute de la décision a été remise par le magistrat signataire.

Vu l'appel interjeté par Franklin L. et la société SMILEY WORLD Ltd. du jugement rendu le 2 mars 2004 par le tribunal de grande instance de Créteil qui a :
- rejeté l'exception d'incompétence soulevée par la société AOL FRANCE,
- rejeté l'exception de nullité de l'assignation,
- débouté Franklin L. et la société SMILEY WORLD Ltd. de l'ensemble de leurs demandes,
- constaté que la marque dénominative « SMILEY » déposée par Franklin L. le 24 juillet 1997, enregistrée sous le N° 97 689 256 n'est pas distinctive pour les services de communication, de télécommunication ou de messageries électroniques,
- prononcé la nullité de cette marque,
- prononcé la déchéance des droits de Franklin L. attachés à l'enregistrement de la marque figurative N° 1 695 775 pour désigner des services de communications ou de transmission de messages, à

compter du 28 décembre 1996,
- prononcé la déchéance des droits de Franklin L. attachés à l'enregistrement de la marque figurative N° 97 668 059 pour désigner des services de télécommunication ou de messageries électroniques, à compter du 7 mars 2002,
- débouté la société AOL FRANCE de ses autres demandes reconventionnelles,
- condamné *in solidum* Franklin L. et la société SMILEY WORLD Ltd. à verser à la société AOL FRANCE la somme de 2 000 euros sur le fondement de l'article 700 du nouveau Code de procédure civile ainsi qu'aux dépens ;

Vu les dernières écritures signifiées le 6 avril 2005 par lesquelles Franklin L. et la société SMILEY WORLD Ltd., poursuivant l'infirmation du jugement entrepris en ce qu'il les a déboutés de leur action en contrefaçon et concurrence déloyale, prononcé la nullité de la marque N° 97 689 256 et la déchéance partielle de leurs droits sur les marques N° 1 695 775 et N° 97 668 775 et sa confirmation pour le surplus, demandent à la Cour de :
- dire que le « visage souriant » diffusé sous la dénomination SMILEY par la société AOL FRANCE sur son site Internet www.aol.com constitue la contrefaçon des marques figuratives N° 1 695 775 et N° 97 668 059 dont Franklin L. est titulaire et propriétaire et la société SMILEY WORLD Ltd. licenciée exclusive,
- dire qu'en diffusant sur son site internet www.aol.com des déclinaisons du « visage souriant » argué de contrefaçon, la société AOL FRANCE a commis des actes de concurrence déloyale et parasitaire à leur encontre,
- ordonner à la société AOL FRANCE de cesser la diffusion du « visage souriant » litigieux et de ses déclinaisons, sous astreinte de 1 000 euros par jour de retard à compter du jour de la signification de l'arrêt à intervenir,
- condamner la société AOL FRANCE à payer les sommes suivantes :
* à Franklin L. 30 000 euros à titre de dommages-intérêts
* à la société SMILEY WORLD Ltd., 30 000 euros à titre de dommages-intérêts,
- les autoriser à faire publier l'arrêt à intervenir, par extraits, dans cinq journaux ou revues de leur choix, aux frais avancés sur simple devis de la société AOL FRANCE jusqu'à hauteur de 20 000 euros HT,
- condamner la société AOL France à leur verser la somme de 10 000 euros sur le fondement de l'article 700 du nouveau Code de procédure civile ;

Vu les dernières conclusions signifiées le 3 mars 2005 aux termes desquelles la société AOL FRANCE sollicite la confirmation du jugement déféré en ce qu'il a débouté Franklin L. et la société SMILEY WORLD de leurs prétentions, prononcé la nullité de la marque N° 97 689 256, prononcé la déchéance partielle des droits de Franklin L. sur les marques N° 1 695 775 et N° 97 668 056 et formant appel incident, prie la Cour de :
- prononcer la nullité de la marque figurative N° 97 668 056 du fait de son caractère usuel et générique pour les services de messageries électroniques au moment de son dépôt,
- constater la dégénérescence de la marque figurative N° 1 695 775,
- condamner solidairement Franklin L. et la société SMILEY WORLD Ltd. à lui verser la somme de 10 000 euros sur le fondement de l'article 700 du nouveau Code de procédure civile ainsi qu'aux dépens ;

SUR QUOI, LA COUR

Considérant que Franklin L. est propriétaire des marques suivantes :
- la marque figurative, déposée le 1er octobre 1971, enregistrée sous le N° 1 695 775, régulièrement renouvelée, représentant la tête stylisée d'un personnage formée d'un cercle entourant deux yeux ronds et une bouche souriante dessinée d'un trait, pour désigner notamment les services de communications et de transmissions de messages,
- la marque figurative, déposée le 7 mars 1997, enregistrée sous le N° 97 668 059, représentant la tête d'un personnage, différent du précédent en ce que le sourire est dessiné par un trait plus creusé, désignant notamment les services de télécommunications, communications par terminaux d'ordinateurs et de messagerie électronique,
- la marque dénominative « SMILEY », déposée le 24 juillet 1997, enregistrée sous le N° 97 689 256, pour désigner notamment les services de télécommunications, de communications par terminaux d'ordinateurs et de messagerie électroniques ;

Que ces marques sont concédées en licence exclusive à la société SMILEY WORLD Ltd. ;

Que reprochant à la société AOL FRANCE d'avoir reproduit sur son site Internet www.aol.com sous la dénomination « SMILEY » des petits visages ronds de couleur jaune souriant ou adoptant d'autres attitudes, qui peuvent être téléchargés, dans le cadre d'un service dénommé AIM, afin d'animer des messages, après avoir fait procéder à un constat d'huissier les 15 et 23 février 2002, Franklin L. et la société SMILEY WORLD l'ont assignée devant le tribunal de grande instance de Créteil aux fins de la voir condamner pour contrefaçon de marques et concurrence déloyale ;

- Sur la demande en nullité de la marque « SMILEY » N° 97 689 256

Considérant qu'après avoir opposé ce signe à la société AOL FRANCE dans le cadre de la présente procédure, Franklin L. a renoncé à l'invoquer pour fonder son action

en contrefaçon ; qu'il soutient que la société AOL FRANCE n'a plus intérêt à en solliciter la nullité ;

Mais considérant que dans leurs dernières écritures, les appelants reprochent à la société AOL FRANCE de faire usage de la dénomination « SMILEY » pour désigner l'icône litigieuse, en l'analysant comme une circonstance de nature à aggraver le risque de confusion ; qu'ils se prévalent donc de droits privatifs sur ce signe de sorte que la société AOL FRANCE justifie d'un intérêt actuel et légitime à en poursuivre la nullité ;

Que cette exception d'irrecevabilité doit donc être rejetée ;

Considérant que la société AOL FRANCE soutient que le terme anglo-saxon « SMILEY » était générique en 1997 pour désigner des services de communication, de télécommunications et de messageries électroniques ; qu'au soutien de cette exception, elle invoque quatre pièces en langue anglaise ;

Mais considérant qu'aucune traduction de ces documents n'est produite aux débats ; qu'en tout état de cause, seul un article intitulé « Who invented the smiley face? » porte une date antérieure au dépôt de la marque ; que cet élément est insuffisant à établir que cette dénomination serait la désignation nécessaire, générique ou usuelle des services de télécommunications ou de messageries électroniques visés au dépôt ;

Que le jugement entrepris doit donc être infirmé en ce qu'il a prononcé la nullité de la marque dénominative N° 97 689 256 ;

- Sur la demande en nullité de la marque N° 97 668 059

Considérant que la société AOL FRANCE soulève la nullité de ce signe pour désigner les services de la classe 38, faisant valoir que les représentations schématiques de visage humain ont commencé à être utilisées dans le domaine de la communication par terminaux d'ordinateurs et, plus particulièrement, celui de la transmission de message électronique à la fin des années 1970 - début des années 1980 ;

Mais considérant que si l'extrait du Guide de l'Internet, édité par la société MICROSOFT France, produit aux débats, daté du 9 juillet 2004, propose de personnaliser les messages en utilisant les caractères du clavier de l'ordinateur pour créer des « *smileys, encore appelés émoticons ou binettes* » parmi lesquels figure le visage souriant évoquant la marque litigieuse, aucun élément ne démontre que ces symboles graphiques avaient déjà cours antérieurement au 7 mars 1997, date du dépôt de la marque ; que la preuve n'est pas davantage rapportée que la version 6.0 du logiciel Word incluait dans son programme Word Office 95 une fonction de correction automatique transformant certains signes en icône « Smiley » ;

Que le caractère générique de la marque n'étant pas établi, le jugement entrepris doit être confirmé en ce qu'il a rejeté l'exception de nullité soulevée par la société AOL France ;

- Sur la déchéance pour défaut d'exploitation des marques figuratives N° 1 695 775 et N° 97 668 059

Considérant qu'il ressort de l'attestation établie par Jason Mc K., vice-président de la société HUNTER SOLUTION, le 21 septembre2004, que la société SMILEY WORLD a ouvert auprès de cet organisme, entre le 15 avril 2000 et le 18 juillet 2001, cinq sites Internet dont le nom intègre la dénomination « SMILEY », qui sont en service permanent depuis leur création ; qu'il précise que deux de ces sites www.smilevworld.com et www.smileyworld.fr offrent un service de E-Mails au public depuis le 1er novembre 2001 et que la société HUNTER SOLUTION a facturé à la société SMILEY WORLD un montant total de 245 513,75 US$ du 18 juillet 2001 jusqu'à avril 2002 ; qu'il ajoute que la société « *HUNTER SOLUTION a facturé un montant de 71 998,72 US$ du 26 mars 2001 jusqu'au 1er mai 2002 pour une campagne de publicité mondiale sur les sites YAHOO et AOL présentant la bannière de publicité de Smileyworld au public de tous pays comprenant la France par le biais des mots-clés suivants : smile, smiley face, yellow face...* » ;

Que les appelants versent aux débats des pages d'écran du site www.smileyworld.com sur lesquelles figurent la représentation du visage souriant de la marque N° 97 668 059 ; que ce site permet de télécharger le logo, objet de la marque, et de disposer d'un service de courrier électronique par l'intermédiaire duquel il est fait usage de ce signe ;

Qu'est également produit aux débats un ouvrage intitulé « Dico Smileys », édité en février 2002 aux Éditions Marabout, sur la dernière de couverture duquel figurent les mentions suivantes :
« Téléchargez les Smileys sur votre portable au … »
« Ouvrez une boîte e-mail gratuite sur le site www.smiley-world.fr » ;

Que cet ouvrage est illustré de représentations graphiques des deux marques litigieuses ;

Considérant que la société SMILEY WORLD a, par ailleurs, conclu le 22 juin 2001 avec la société SKY

MEDIA un contrat de concession de licence relatif à l'exploitation de la marque « Vignette sourire » N° 97 668 059 l'autorisant à reproduire cette marque sur les écrans de téléphone mobile ; que ce service a donné lieu à une campagne publicitaire dans les magazines de télévision, comme en atteste le numéro de « TV Magazine LE FIGARO » daté du 24 novembre 2001 ; que ces logos peuvent être utilisés, non seulement comme fond d'écran, mais adressés à d'autres personnes pour délivrer un message notamment par SMS, comme prévu au contrat ;

Considérant que, contrairement aux assertions de la société AOL FRANCE, ces éléments établissent un usage de la marque figurative N° 97 668 059 pour des services de télécommunications, de communications par terminaux d'ordinateurs et de messageries électroniques impliquant l'établissement d'une relation avec autrui, non limité à un service de publication proposant des images ; que la société AOL FRANCE le reconnaît d'ailleurs en mentionnant sur son propre site, le site www.smileydictionary.com pour indiquer qu'il propose environ 1 000 *emoticons* et explique comment s'en servir ;

Qu'il s'agit bien d'un usage à titre de marque dès lors que le logo représentant le visage souriant précède ou accompagne le nom du site ; qu'il en est de même pour son utilisation pour la communication par les téléphones mobiles, ce logo figurant sur les publicités en faveur de ce service ;

Considérant que Franklin L. justifie donc d'un usage réel et sérieux de la marque N° 97 668 059, pour les services de la classe 38, de nature à faire échec à l'exception de déchéance ;

Considérant que la marque figurative N° 1 695 775 ne diffère de la marque N° 97 668 059 que par le graphisme de la bouche qui accuse un sourire plus épanoui ;

Que l'usage de cette marque, sous la forme modifiée objet de l'enregistrement N° 97 668 059, qui vient d'être examiné, n'en altère pas le caractère distinctif de sorte qu'il répond aux conditions exigées par l'article L.714-5 alinéa 2-b) du Code de la propriété intellectuelle ;

Que le jugement entrepris doit donc être infirmé en ce qu'il a fait droit à l'exception de déchéance ;

- Sur la déchéance de la marque N° 1 695 775 pour dégénérescence

Considérant que la société AOL FRANCE fait valoir, à l'appui de cette exception, que la vignette représentant un visage souriant est devenue un signe couramment utilisé par les internautes, le titulaire de la marque ayant, pendant de nombreuses années, toléré cet usage générique sans réagir ;

Mais considérant que les premiers juges ont relevé à juste titre que la société AOL FRANCE ne produit aucune pièce au soutien de ces allégations ; qu'en outre, Franklin L. et la société SMILEY WORLD justifient, par les copies de jugements et d'arrêts produits aux débats, avoir défendu la marque en cause dès lors que le logo utilisé par les tiers en reproduisait les caractéristiques, au-delà de la simple stylisation d'un visage souriant ;

Qu'il s'ensuit que le jugement a, à juste titre, écarté l'exception tirée de l'article L.714-6-a) du Code de la propriété intellectuelle ;

- Sur la contrefaçon

Considérant que Franklin L. et la société SMILEY WORLD reprochent à la société AOL France d'avoir commis des actes de contrefaçon par imitation des deux marques figuratives précitées en offrant un service dénommé AIM permettant de télécharger des icônes reproduisant des visages ronds stylisés de couleur jaune souriant ou adoptant d'autres attitudes ;

Considérant qu'il ressort du procès-verbal de constat dressé les 15 et 23 février 2002 sur le site www.aol.com.messager que l'icône dite « émoticônes » présentée accompagnée de la signification « Je suis content » reproduit les caractéristiques des deux marques invoquées, à savoir :
- une tête constituée d'un cercle,
- des yeux représentés par deux points noirs en forme d'ovale, et non par des signes + comme le prétend à tort la société AOL FRANCE,
- une bouche formée d'un trait en arc de cercle barré à ses extrémités de deux traits obliques formant les commissures ;

Que si la bouche est légèrement entrouverte, cette différence de détail n'affecte pas l'impression d'ensemble identique qui se dégage de l'examen des deux logos ; qu'il importe peu que cette icône soit présentée parmi un ensemble de visages stylisés décrivant des humeurs, dès lors que chacun d'eux peut être utilisé séparément ;

Que si les appelants ne peuvent se prévaloir de la couleur jaune qui n'est pas revendiquée, l'adoption de ce signe graphique pour désigner des services identiques à ceux visés dans le libellé de l'enregistrement est de nature à laisser accroire au

public qu'ils ont la même origine ou qu'ils sont fournis par des sociétés liées économiquement ;

Que toutefois la protection accordée à ce signe ne peut s'étendre à toute représentation d'un visage rond stylisé quel qu'en soit l'expression ;

Que l'icône destinée à illustrer le texte « Je suis content » constitue donc la contrefaçon par imitation des marques N° 1 695 775 et N° 97 668 059 appartenant à Franklin L.

- Sur la concurrence déloyale

Considérant qu'en faisant usage illicitement et sans bourse délier de ces marques sur lesquelles la société SMILEY WORLD bénéficie de licences exclusives d'exploitation, la société AOL France a commis, à son encontre, une faute engageant sa responsabilité civile ;

- Sur les mesures réparatrices

Considérant que l'atteinte portée à la valeur patrimoniale de ces deux marques du fait de l'usage illicite qu'en a fait la société AOL FRANCE sera entièrement réparé par l'allocation à Franklin L. d'une indemnité de 15 000 euros à titre de dommages-intérêts ;

Que la société SMILEY WORLD, qui n'a pu négocier les conditions d'utilisation de ces signes sur lesquels elle jouit d'un monopole d'exploitation, sur le site Internet de la société AOL FRANCE, a été nécessairement privée d'une perte de gains qui sera évaluée à la somme indemnitaire de 25 000 euros ;

Qu'afin de mettre un terme à ces agissements illicites, il sera fait droit à la demande d'interdiction, selon les modalités précisées au dispositif ; que la mesure de publication sollicitée apparaît également justifiée ;

Considérant que les dispositions de l'article 700 du nouveau Code de procédure civile doivent bénéficier à Franklin L. et à la société SMILEY WORLD, la somme de 10 000 euros devant leur être allouée à ce titre ;

Que la solution du litige commande de rejeter tant la demande de dommages-intérêts pour procédure abusive formée par la société AOL FRANCE que sa demande fondée sur les dispositions de l'article 700 du nouveau Code de procédure civile ;

PAR CES MOTIFS

Confirme le jugement entrepris en ce qu'il a :
- déclaré recevable l'action en nullité de la marque N° 97 689 256,
- débouté la société AOL FRANCE de ses demandes en nullité des marques figuratives N° 1 695 775 et N° 97 668 059,

L'infirmant pour le surplus et statuant à nouveau,

Déboute la société AOL FRANCE de sa demande en nullité de la marque dénominative « SMILEY » N° 97 689 256,

Rejette l'exception de déchéance des droits attachés aux marques N° 97 668 059 et N° 1 695 775 tant pour défaut d'exploitation que pour dégénérescence,

Dit qu'en reproduisant et diffusant sur son site Internet www.aol.com l'icône représentant un visage souriant, illustrant le texte « Je suis content », la société AOL FRANCE a commis des actes de contrefaçon par imitation des marques N° 1 695 775 et N° 97 668 059 dont Franklin L. est propriétaire et a commis des actes de concurrence déloyale au détriment de la société SMILEY WORLD, titulaire de licences exclusives sur ces deux marques,

Fait interdiction à la société AOL FRANCE de faire usage de cette icône, sous astreinte de 500 euros par jour de retard à compter de la signification du présent arrêt,

Condamne la société AOL FRANCE à payer les sommes suivantes :
- 15 000 euros à titre de dommages-intérêts à Franklin L. en réparation des actes de contrefaçon,
- 25.000 euros à titre de dommages-intérêts à la société SMILEY WORLD en réparation des actes de concurrence déloyale,

Autorise Franklin L. et la société SMILEY WORLD à publier le dispositif du présent arrêt, en entier ou par extraits, dans trois journaux ou revues de leur choix, aux frais de la société AOL FRANCE, dans la limite globale de 9 000 euros HT,

Rejette le surplus des demandes, condamne la société AOL FRANCE à verser à Franklin L. et à la société SMILEY WORLD une somme de 10 000 euros sur le fondement de l'article 700 du nouveau Code de procédure civile,Condamne la société AOL FRANCE aux dépens qui pourront être recouvrés conformément à l'article 699 du nouveau Code de procédure civile. »

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

TGI Paris, ordonnance de référé du 08 juillet 2005, REAL MADRID CLUB DE FOOTBALL, ZINEDINE Z. ET AUTRES C/ HILTON GROUP PLC, SPORTING EXCHANGE LTD. ET AUTRES

Thèmes
Loi applicable et juridiction compétente, Droits de la personnalité
Abstract
Paris sportif, sites sont accessibles aux internautes français, article 31 et 5.3 du règlement (CE) n° 44/2001, droit à l'image, droit au nom, promotion commerciale (non) trouble manifestement illicite (non)
Résumé
Un club de football est ses joueurs cherchent à empêcher des sociétés de paris en ligne d'utiliser leur noms dans le cadre de leur activité
Décision

DEMANDEURS
REAL MADRID CLUB DE FOOTBALL
Monsieur Zinedine Z.
Monsieur David B.
Monsieur Raul G.
Monsieur Ronaldo N.
Monsieur Luis M.
Représentés par la SCP STASI & ASSOCIES et Me Jean-Louis DUPONT

DEFENDERESSES
HILTON GROUP PLC
Société SPORTING EXCHANGE LTD
William H.
SPORTINGBET PLC
Représentées par Me Grégoire TRIET
MRBOOKMAKER.COM LTD
Représentée par Me Etienne WERY, Me Thibault VERBIEST et Me Paul VAN DEN BULCK

INTERVENANTES VOLONTAIRES
WILLIAM HILL CREDIT LIMITED
LADBROKES LTD.
Représentées par Me Grégoire TRIET
INTERNET OPPORTUNITY ENTERTAINMENT LTD
Représentée par SCP BIGNON LEBRAY DELSOL & ASSOCIES

Nous, Président,

Après avoir entendu les parties comparantes ou leur conseil,

Vu les actes introductifs du présent référé délivrés les 24 mars 2005 à la requête de l'Association sportive REAL MADRID CLUB DE FOOTBALL et de Messieurs Zinedine Z., David B., Raul G., Ronaldo N., et Luis Filipe M. à l'encontre des sociétés de droit anglais HILTON GROUP PLC, SPORTING EXCHANGE LTD., SPORTINGBET PLC, William H. et la société MRBOOKMAKER.COM LTD. établie à MALTE ;

Vu les dernières conclusions déposées le 16 juin par les requérants aux termes desquelles ils demandent au juge des référés, sur le fondement des articles 9 du Code civil et 809 alinéa 1er du nouveau Code de procédure civile de :
- dire la société REAL MADRID et les joueurs de football susvisés recevables et bien fondés en leur action ;
- constater la violation du droit à l'image et au nom des joueurs concernés ;
- dire que cette violation est constitutive d'un trouble manifestement illicite qu'il convient de faire cesser ;

En conséquence,
- prononcer à l'égard des Sociétés HILTON GROUP PLC, SPORTING EXCHANGE LTD., SPORTINGBET PLC, WILLIAM HILL, WILLIAM CREDIT LIMITED, LADBROKES LTD., MRBOOKMAKER.COM LTD., INTERNET OPPORTUNITY ENTERTAINMENT LTD., l'interdiction immédiate de toute utilisation du nom et de l'image de Messieurs Zinedine Z., David B., Raul G., Ronaldo N., et Luis M. joueurs du REAL MADRID, sans autorisation dans le cadre de la promotion et l'organisation de paris sur internet ;
- assortir cette interdiction d'une astreinte de 50.000 euros pour chaque utilisation sans autorisation du nom ou de l'image des joueurs concernés constatée à compter de la décision à intervenir ;
- débouter les sociétés défenderesses de toutes leurs prétentions ;
- condamner en outre les sociétés défenderesses à payer à la société REAL MADRID et chacun des joueurs la somme de 10.000 euros H.T. au titre de l'article 700 du nouveau Code de procédure civile ainsi qu'aux entiers dépens ;

Vu les conclusions prises le 16 juin 2005 par les sociétés de droit anglais HILTON GROUP PLC, SPORTING EXCHANGE Ltd, défenderesses et par les sociétés de droit anglais WILLIAM HILL CREDIT LIMITED et LADBROKES Ltd. intervenantes volontaires qui demandent au juge des référés de :

<u>À titre principal :</u>
- se déclarer incompétent au profit des juridictions britanniques compétentes ;

À titre subsidiaire :
- mettre les sociétés HILTON GROUPE PLC, et SPORTINGBET PLC hors de cause ;
- déclarer les sociétés WILLIAM HILL CREDIT LIMITED et LADBROKES Ltd. recevables et bien fondées en leurs interventions volontaires ;
- déclarer la société REAL MADRID CLUB DE FOOTBALL irrecevables en l'ensemble de ses demandes ;
- dire que l'utilisation des noms de Messieurs Zinedine Z., David B., Raul G., Ronaldo N., et Luis M. pour les désigner en tant que joueurs participant à des matchs de football publics, sur les sites internet « willhill.com »« ladbrokes.com »et « betfair.com »ne porte pas atteinte à leur vie privée ;

En conséquence :
- constater l'absence de trouble manifestement illicite et dire n'y avoir lieu à référé ;
- débouter la société REAL MADRID CLUB DE FOOTBALL, Messieurs Zinedine Z., David B., Raul G., Ronaldo N., et Luis Filipe M. de l'ensemble de leurs demandes ;

À titre infiniment subsidiaire,
- dire que dans l'hypothèse d'une condamnation des défenderesses, l'interdiction ne pourrait qu'être limitée au territoire français ;
- dire que dans ce cas, les défenderesses disposeront d'un délai de 30 jours ouvrables à compter de la signification de l'ordonnance à intervenir pour modifier leurs sites ;

En toute hypothèse,
- condamner chacun des demandeurs à verser à chacune des sociétés la somme de 15.000 euros au titre de l'article 700 du nouveau Code de procédure civile ainsi qu'aux dépens ;

Vu les conclusions déposées le 16 juin 2005 par la société INTERNET OPPORTUNITY ENTERTAINMENT LTD., intervenante volontaire, qui demande au juge des référés de :
- se déclarer incompétent au profit de la juridiction antiguaise compétente ;

À titre subsidiaire,
- déclarer la société INTERNET OPPORTUNITY ENTERTAINMENT LTD. recevable et bien fondée en son intervention volontaire ;
- déclarer la société REAL MADRID CLUB DE FOOTBALL irrecevable en l'ensemble de ses demandes ;
- constater l'absence de trouble manifestement illicite et dire n'y avoir lieu à référé ;
- dire que l'utilisation des noms de Messieurs Zinedine Z., David B., Raul G., Ronaldo N., et Luis M. pour les désigner en tant que joueurs participant à des matchs de football public, sur le site internet miapuesta.com ne porte pas atteinte à leur vie privée et encore moins à l'intimité de leur vie privée ;
- dire que l'utilisation des mêmes joueurs sur le site miapuesta.com pour illustrer un match de football à venir, ne porte pas atteinte à leur vie privée et encore moins à l'intimité de leur vie privée ;
- débouter la société REAL MADRID CLUB DE FOOTBALL, Messieurs Zinedine Z., David B., Raul G., Ronaldo N., et Luis M. de l'ensemble de leurs demandes ;

À titre infiniment subsidiaire,
- dire que dans l'hypothèse d'une condamnation de la société INTERNET OPPORTUNITY ENTERTAINMENT Ltd., l'interdiction ne pourrait qu'être limitée au territoire français ;
- dire que dans cette hypothèse, la société INTERNET OPPORTUNITY ENTERTAINMENT Ltd. disposera d'un délai de trente jours ouvrables à compter de la signification de l'ordonnance à intervenir pour modifier son site ;

En toute hypothèse,
- condamner les demandeurs aux entiers dépens ;

Vu les conclusions du 16 juin 2005 par lesquelles la société MRBOOKMAKER.COM LTD. soulève à titre principal la nullité de l'assignation qui lui a été délivrée ;

À titre subsidiaire, il demande au juge des référés de se déclarer incompétent au profit des juridictions de la République démocratique de MALTE, ou à défaut, poser à la Cour de Justice des Communautés européennes la question préjudicielle reproduite dans le dispositif de ses écritures et plus encore subsidiairement, renvoyer la question de la compétence au juge du fond ;

À titre plus subsidiaire,
- déclarer le REAL MADRID irrecevable en sa demande ;
- déclarer la demande non fondée en ce qu'elle repose sur les dispositions du droit français, inapplicable en l'espèce ;
Ou, à défaut sur l'application du droit français, poser à la Cour de Justice des Commmunautés européennes la question préjudicielle mentionnée dans le dispositif de ses écritures ;

À titre infiniment subsidiaire,
- constater l'absence de trouble manifestement illicite et dire n'y avoir lieu à référé ;
- déclarer la société REAL MADRID CLUB DE FOOTBALL, Messieurs Zinedine Z., David B., Raul G., Ronaldo N, et Luis M. de l'ensemble de leurs demandes ;

À titre le plus subsidiaire (sic),
- dire que dans l'hypothèse d'une condamnation des défenderesses, l'interdiction est limitée au territoire français ;
- dire que dans cette hypothèse, elle disposera d'un délai

de trente jours ouvrables à compter de la signification de l'ordonnance à intervenir pour modifier son site ;

En toute hypothèse,
- condamner chacun des demandeurs à lui verser les sommes de 100.000 euros en réparation de l'abus de procédure qu'ils ont commis et de 15.000 euros au titre de l'article 700 du nouveau Code de procédure civile ;
- condamner les demandeurs aux entiers dépens ;

SUR CE :

1. Sur la nullité de l'assignation délivrée à la société MRBOOKMAKER.COM LTD. :

Attendu qu'à l'appui de son exception de nullité la société MRBOOKMAKER.COM LTD. expose que l'assignation a été délivrée à cinq sociétés distinctes qui n'ont aucun lien entre elles, si ce n'est qu'elles exercent, en partie le même métier ; qu'il n'est allégué à l'encontre des défenderesses ni une démarche concertée ou collective, ni faits communs ; qu'elle dénonce le procédé qui est contraire au principe constitutionnel et international du droit à un procès équitable et revendique le droit d'être jugée pour sa propre cause et ses propres faits ;

Attendu qu'il doit tout d'abord être constaté que l'assignation délivrée à la société MRBOOKMAKER.COM LTD. satisfait aux exigences de l'article 56 du nouveau Code de procédure civile ;

Attendu en outre que si, l'assignation a été délivrée à plusieurs défendeurs qui n'ont effectivement aucun lien juridique entre eux, il apparaît que l'objet et le fondement des prétentions des requérants sont identiques à l'égard de chacun d'eux ; que ce mode d'introduction du présent référé ne saurait en aucun cas priver les défendeurs du droit à un procès équitable dès lors que le juge a l'obligation d'examiner respectivement les faits imputés à chacun d'entre eux et répondre aux moyens de défense qui leur sont propres ;

Attendu qu'il suit que l'exception de nullité soulevée par la société MRBOOKMAKER.COM LTD sera rejetée ;

Sur l'intervention volontaire des sociétés de droits anglais WILLIAM HILL CREDIT LIMITED et LADBROKES LTD. :

Attendu que les sociétés de droits anglais WILLIAM HILL CREDIT Ltd. et LADBROKES LTD. qui exploitent respectivement les sites « Willhill.com » et « Ladbrokes.com » justifient d'un intérêt à agir pour s'opposer aux mesures d'interdiction sollicitée par les requérants ; que leur intervention volontaire sera donc déclarée recevable ;

Sur l'intervention volontaire de la société de droit antiguais INTERNET OPPORTUNIY ENTERTAINMENT LTD. :

Attendu que la société de droit antiguais INTERNET OPPORTUNITY ENTERTAINMENT LTD. dont il n'est pas discuté qu'elle est propriétaire du site internet « www.miapuesta.com » a intérêt à agir pour défendre son exploitation ; que son intervention volontaire sera également déclarée recevable ;

Sur l'exception d'incompétence :

Attendu que les requérants exposent que les sociétés défenderesses et intervenantes volontaires exploitent sur leurs sites internet hébergés à l'étranger une activité de paris en ligne portant notamment sur les matchs de football du championnat d'Espagne en utilisant leurs images de footballeurs professionnels ainsi que leurs noms ; que ces sites sont accessibles aux internautes français lesquels peuvent se connecter et, le cas échéant, parier ;

Attendu que s'agissant des sociétés de droit anglais dont les sites sont hébergés dans cet État, ainsi que de la société MRBOOKMAKER.COM Ltd. établie à MALTE, les dispositions de l'article 31 du règlement (CE) n° 44/2001 du Conseil de l'Union Européenne, dont il n'est pas discuté qu'elles leurs sont applicable prévoient « *que les mesures provisoires ou conservatoires prévues par la loi d'un État membre peuvent être demandées aux autorités judiciaires de cet État, même si, en vertu du présent règlement, une juridiction d'un autre État membre est compétente pour connaître du fond* » ;

Que par ailleurs l'article 5.3 de ce même règlement dispose qu'une personne domiciliée sur le territoire d'un État membre peut être attraite dans un autre État membre, en matière délictuelle ou quasi délictuelle, devant le tribunal du lieu où le fait dommageable s'est produit ou risque de se produire ;

Attendu qu'il découle de la combinaison de ces textes, alors qu'il est établi que les faits dommageables allégués se sont produits ou sont susceptibles de se produire sur le territoire national dès lors que les internautes français peuvent se connecter sur les sites susvisés et consulter les messages et images litigieux, le juge des référés français est compétent pour prescrire, s'il y a lieu, les mesures provisoires sollicitées ; qu'il est sans effet que le nombre de parieurs soit très réduit ainsi que l'invoquent les défendeurs ;

Attendu que pour ce qui est de la société de droit antiguais INTERNET OPPORTUNITY ENTERTAINMENT LTD., laquelle admet dans ses écritures que les règles de procédure civile française lui

sont applicables, la matérialité du dommage allégué par les requérants sur le territoire national est tout aussi établie à son encontre pour les mêmes motifs ;

Attendu qu'il convient en conséquence, sans qu'il soit nécessaire de poser la question préjudicielle à la Cour de Justice de la Communauté Européenne demandée par la Société MRBOOKMAKER.COM LTD., de rejeter les exceptions d'incompétence ;

Attendu que l'utilisation des images de Messieurs Zinedine Z. et David B., consistant à l'évidence dans la reproduction d'une photographie d'un match disputé par eux, n'est directement associé par les sociétés mises en cause à promouvoir leur activité de paris ; qu'elle sert de présentation du match sur lequel le pari est organisé ;

Attendu que l'utilisation des noms de Messieurs Zinedine Z., David B., Raul G., Ronaldo N., et Luis M. n'est pas davantage associée à la promotion des paris ; que de la même manière, elle rappelle aux éventuels parieurs les noms des joueurs de football, certes les plus célèbres, qui sont appelés à disputer la rencontre ;

Attendu qu'il n'est pas démontré dans ces conditions avec l'évidence exigée en référé que l'utilisation desdites photographies et la citation des noms des joueurs susvisés qui est en rapport direct avec leur activité professionnelle, constitue une atteinte caractérisée à leurs droits ;

Qu'il n'appartient qu'au juge du fond de se prononcer sur le litige opposant les parties ;

Attendu qu'il n'y a pas lieu en l'absence de trouble manifestement démontré par les requérants de prescrire les mesures provisoires sollicitées par eux ;

Attendu qu'il n'est pas démontré un abus de la part des requérants dans l'exercice de leur droit d'agir en justice ; que la demande de dommages-intérêts formée de ce chef par la société MRBOOKMAKER.COM sera rejetée ;

Attendu en revanche que les requérants qui succombent sur leurs demandes seront condamnés *in solidum* aux dépens ;

Attendu que l'équité ne commande pas de faire application des dispositions de l'article 700 du nouveau Code de procédure civile au profit tant des sociétés défenderesses que des sociétés intervenantes volontaires ayant sollicité le bénéfice de ce texte ;

PAR CES MOTIFS

Statuant publiquement en premier ressort, par ordonnance contradictoire,

Déclarons recevables les interventions volontaires des sociétés de droit anglais WILLIAM HILL CREDIT LTD. et LADBROKES LTD. ainsi que la société de droit antiguais INTERNET OPPORTUNITY ENTERTAINMENT LTD. ;

Prononçons la mise hors de cause des sociétés HILTON GROUPE PLC. et SPORTINGBET PLC. ;

Rejetons l'exception de nullité de l'assignation soulevée par la société MRBOOKMAKER.COM LTD. ;

Rejetons les exceptions d'incompétence ;

Disons n'y avoir lieu à référé sur l'ensemble des requérants ;

Déboutons la société MRBOOKMAKER.COM LTD. de sa demande de dommages-intérêts pour procédure abusive ;

Disons n'y avoir lieu à l'application de l'article 700 du nouveau Code de procédure civile au profit tant des sociétés défenderesse que des sociétés intervenantes volontaires ;

Rejetons toute autre demande ;

Condamnons *in solidum* les requérants aux entiers dépens. »

Référence : Tribunal de Grande Instance de Paris, ordonnance de référé du 08 juillet 2005, REAL MADRID CLUB DE FOOTBALL, ZINEDINE Z. ET AUTRES C/ HILTON GROUP PLC, SPORTING EXCHANGE LTD. ET AUTRES, RDTIC n°48.
http://www.droit-tic.com/juris/aff.php?id_juris=53

DROIT-TIC.com

R.D.T.I.C

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

TEXTES OFFICIELS

INFORMATIQUE ET LIBERTÉS, VIE PRIVÉE

DÉCRET N° 2005-1726 DU 30 DÉCEMBRE 2005 RELATIF AUX PASSEPORTS ÉLECTRONIQUES

Par Julien Le Clainche, Allocataire de recherche

Décret n° 2005-1726 du 30 décembre 2005 relatif aux passeports électroniques , J.O n° 304 du 31 décembre 2005 page 20742, texte n° 15.

Décret n° 2005-1726 du 30 décembre 2005 relatif aux passeports électroniques

J.O n° 304 du 31 décembre 2005 page 20742
texte n° 15

Décrets, arrêtés, circulaires
Textes généraux
Ministère de l'intérieur et de l'aménagement du territoire
NOR: INTD0500343D

Le Premier ministre,

Sur le rapport du ministre d'Etat, ministre de l'intérieur et de l'aménagement du territoire, et du ministre des affaires étrangères,

Vu la Convention du 19 juin 1990 d'application de l'accord signé à Schengen le 14 juin 1985 entre les gouvernements des Etats de l'Union économique du Benelux, de la République fédérale d'Allemagne et de la République française relatif à la suppression graduelle des contrôles aux frontières communes, dont la ratification a été autorisée par la loi n° 91-737 du 30 juillet 1991, notamment ses articles 2 et 100 ;

Vu le règlement (CE) n° 2252/2004 du 13 décembre 2004 du Conseil ;

Vu la position commune 2005/69 JAI du Conseil du 24 janvier 2005 ;

Vu le code civil ;

Vu le code général des impôts, notamment son article 953 ;

Vu le décret de la Convention nationale du 7 décembre 1792 relatif aux passeports à accorder à ceux qui seraient dans le cas de sortir du territoire français pour leurs affaires ;

Vu la loi du 14 ventôse an IV qui détermine le mode de délivrance des passeports à l'étranger ;

Vu la loi n° 69-3 du 3 janvier 1969 modifiée relative à l'exercice des activités ambulantes et au régime applicable aux personnes circulant en France sans domicile ni résidence fixe ;

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

Vu l'arrêté des consuls de la République du 12 messidor an VIII qui détermine les fonctions du préfet de police à Paris, notamment son article 3 ;

Vu le décret n° 55-1397 du 22 octobre 1955 modifié instituant la carte nationale d'identité ;

Vu le décret n° 62-921 du 3 août 1962 modifié modifiant certaines règles relatives aux actes de l'état civil, et notamment son article 11 ;

Vu le décret n° 93-1362 du 30 décembre 1993 relatif aux déclarations de nationalité, aux décisions de naturalisation, de réintégration, de perte, de déchéance et de retrait de la nationalité française, modifié par les décrets n° 98-720 du 20 août 1998 et n° 2005-25 du 14 janvier 2005 ;

Vu le décret n° 97-1191 du 19 décembre 1997 pris pour l'application au ministre de l'intérieur du 1° de l'article 2 du décret n° 97-34 du 15 janvier 1997 relatif à la déconcentration des décisions administratives individuelles ;

Vu le décret n° 2001-847 du 11 septembre 2001 relatif à la durée des passeports délivrés en Nouvelle-Calédonie, en Polynésie française, dans les îles Wallis et Futuna, à Mayotte et à Saint-Pierre-et-Miquelon ;

Vu le décret n° 2003-1377 du 31 décembre 2003 relatif à l'inscription au registre des Français établis hors de France, modifié par le décret n° 2005-302 du 30 mars 2005 ;

Vu le décret n° 2004-1543 du 30 décembre 2004 relatif aux attributions des chefs de postes consulaires en matière de titres de voyage, modifié par le décret n° 2005-851 du 27 juillet 2005 ;

Vu l'avis de la Commission nationale de l'informatique et des libertés en date du 22 novembre 2005 ;

Le Conseil d'Etat (section de l'intérieur) entendu,

Décrète :

TITRE Ier : DISPOSITIONS GÉNÉRALES

Chapitre Ier : Dispositions communes au passeport électronique, au passeport électronique de service et au passeport électronique de mission

Article 1

Le passeport électronique, le passeport électronique de service et le passeport électronique de mission mentionnent :

- le nom de famille, les prénoms dans l'ordre de l'état civil, la date et le lieu de naissance, le sexe et, si l'intéressé le demande, le nom dont l'usage est autorisé par la loi ;

- la couleur des yeux, la taille ;

- la nationalité ;

- le domicile ou la résidence ou, le cas échéant, la commune de rattachement de l'intéressé ou l'adresse de l'organisme d'accueil auprès duquel il est domicilié ;

- la date de délivrance et la date d'expiration du document, ainsi que l'autorité qui l'a délivré ;

- le numéro du passeport.

Ils comportent également la signature manuscrite et l'image numérisée de leur titulaire.

Ils certifient l'identité de leur titulaire.

Article 2

Afin de faciliter l'authentification du détenteur des passeports mentionnés à l'article 1er, ces titres comportent un composant électronique contenant les données mentionnées au même article, à l'exception de la signature.

Ce composant électronique, qui est une puce sans contact, comporte des sécurités de nature à prémunir le titulaire du titre contre les risques d'intrusion, de détournement et de modification.

Article 3

Afin de faciliter l'identification du détenteur des passeports mentionnés à l'article 1er et l'authentification de ces titres, ces titres comportent une zone de lecture optique contenant les informations suivantes : le nom de famille, le ou les prénoms, le sexe, la date de naissance et la nationalité du titulaire, le type de document, l'Etat émetteur, le numéro du titre et sa date d'expiration.

Chapitre II : Conditions de délivrance et de renouvellement du passeport électronique

Article 4

Le passeport électronique est délivré, sans condition d'âge, à tout Français qui en fait la demande.

Il a une durée de validité de dix ans. Lorsqu'il est délivré à un mineur, sa durée de validité est de cinq ans.

Article 5

Le passeport électronique est délivré ou renouvelé sur production de la copie intégrale d'un des actes de l'état civil figurant sur une liste déterminée par arrêté du ministre de l'intérieur.

La preuve de la nationalité française du demandeur est établie à partir de l'un des actes de l'état civil visés à l'alinéa précédent, portant le cas échéant, en marge, l'une des mentions prévues à l'article 28 du code civil.

Lorsque les actes de l'état civil visés au deuxième alinéa ne suffisent pas à établir la qualité de Français du demandeur, celle-ci peut être établie par la production de l'une des pièces justificatives de la nationalité française mentionnées aux articles 34 et 52 du décret du 30 décembre 1993 susvisé ou d'un certificat de nationalité française.

Le demandeur fournit deux photographies d'identité de format 35 x 45 mm, identiques, récentes et parfaitement ressemblantes, le représentant de face et tête nue.

Le demandeur justifie s'être acquitté du droit de timbre prévu par la loi.

Article 6
Le demandeur justifie de son domicile ou de sa résidence par tous moyens, notamment par la production d'un titre de propriété, d'un certificat d'imposition ou de non-imposition, d'une quittance de loyer, de gaz, d'électricité, de téléphone ou d'une attestation d'assurance du logement.

Le demandeur auquel la loi a fixé une commune de rattachement produit un livret spécial de circulation, un livret de circulation ou un carnet de circulation en cours de validité.

Le demandeur qui n'a pas la possibilité d'apporter la preuve d'un domicile ou d'une résidence, ou auquel la loi n'a pas fixé une commune de rattachement, fournit une attestation établissant son lien avec un organisme d'accueil figurant sur une liste établie par le préfet et, à Paris, par le préfet de police.

Article 7
Lorsque le passeport est demandé pour remplacer un passeport perdu ou volé, le demandeur produit, en outre, une déclaration de perte ou de vol.

Article 8
La demande de passeport faite au nom d'un mineur est présentée par une personne exerçant l'autorité parentale.

La demande de passeport faite au nom d'un majeur placé sous tutelle est présentée par son tuteur.

Dans l'un et l'autre cas, le représentant légal doit justifier de sa qualité.

Article 9
Le passeport électronique est délivré ou renouvelé par le préfet ou le sous-préfet.

A Paris, il est délivré ou renouvelé par le préfet de police.

A l'étranger, il est délivré ou renouvelé par le chef de poste consulaire.

Article 10
Le passeport est remis au demandeur au lieu de dépôt de la demande. Le demandeur signe le passeport en présence de l'agent qui le lui remet.

Le passeport d'un mineur lui est remis en présence d'une personne exerçant l'autorité parentale.

Article 11
Lors du renouvellement, le nouveau passeport est remis après restitution de l'ancien passeport.

L'ancien passeport peut être conservé par le demandeur dans le cas où il comporte un visa en cours de validité pour la durée de validité de ce visa.

Article 12
Le demandeur est informé de la mise à disposition du passeport par tout moyen. Tout passeport non retiré par l'intéressé, dans le délai de trois mois suivant sa mise à disposition par l'autorité auprès de laquelle la demande a été déposée, est détruit.

Chapitre III : Conditions de délivrance et de renouvellement du passeport électronique de service

Article 13
Un passeport de service peut être délivré :

1° Aux agents civils et militaires de l'Etat qui effectuent à l'étranger des missions sur ordre, présentant un intérêt national, pour le compte exclusif d'une administration centrale, et qui ne sont pas titulaires d'un passeport diplomatique ;

2° Aux agents civils et militaires de l'Etat affectés à l'étranger, attachés à une mission diplomatique permanente ou à un poste consulaire, et qui ne sont pas titulaires d'un passeport diplomatique ;

3° Au conjoint ou partenaire auquel il est lié par un pacte civil de solidarité et aux enfants mineurs à charge des agents mentionnés au 2° lorsque les circonstances locales nécessitent la délivrance d'un tel titre.

Le passeport de service a une durée de validité de cinq ans.

Article 14
La demande de passeport de service est déposée

auprès du ministre de l'intérieur.

Elle est accompagnée d'une note circonstanciée établie par l'administration dont relève l'agent justifiant la nécessité de délivrer un passeport de service.

En cas d'affectation à l'étranger de l'intéressé, la décision portant nomination de l'agent est produite à l'appui de la demande.

Le passeport de service est délivré par le ministre de l'intérieur.

Le passeport de service ne peut être utilisé qu'aux fins pour lesquelles il est délivré.

Il est restitué par l'administration dont relève le titulaire à l'expiration de sa validité ou dès lors que son utilisation n'est plus justifiée.

Chapitre IV : Conditions de délivrance et de renouvellement du passeport électronique de mission

Article 15
Un passeport de mission peut être délivré aux agents civils et militaires de l'Etat qui se rendent en mission à l'étranger ou sont affectés à l'étranger et ne sont pas titulaires d'un passeport diplomatique ou d'un passeport de service.

Le passeport de mission a une durée de validité de cinq ans.

Article 16
Le passeport de mission est délivré :

- par le préfet ou le sous-préfet ;

- à Paris, par le préfet de police ;

- à l'étranger, par le chef de poste consulaire.

Article 17
La demande de passeport de mission est accompagnée d'un ordre de mission signé par l'autorité exerçant le pouvoir hiérarchique à l'égard du demandeur.

Le passeport de mission ne peut être utilisé qu'aux fins pour lesquelles il a été délivré.

Le passeport de mission est restitué à l'autorité qui l'a délivré à l'expiration de sa validité ou dès lors que son utilisation n'est plus justifiée.

TITRE II : DISPOSITIONS RELATIVES AU TRAITEMENT AUTOMATISÉ DES DONNÉES À CARACTÈRE PERSONNEL RELATIF À LA DÉLIVRANCE DU PASSEPORT ÉLECTRONIQUE, DU PASSEPORT ÉLECTRONIQUE DE SERVICE ET DU PASSEPORT ÉLECTRONIQUE DE MISSION

Article 18
Afin de mettre en oeuvre les procédures d'établissement, de délivrance, de renouvellement, de remplacement et de retrait des passeports mentionnés à l'article 1er, ainsi que pour prévenir, détecter et réprimer leur falsification et leur contrefaçon, le ministre de l'intérieur est autorisé à créer un système de traitement automatisé de données à caractère personnel.

Article 19
Les données à caractère personnel enregistrées dans le système de traitement automatisé prévu à l'article 18 sont :

a) Les données relatives au titulaire du passeport :

- le nom de famille, les prénoms et, si le requérant le demande, le nom dont l'usage est autorisé par la loi, la date et le lieu de naissance, le sexe ;

- la couleur des yeux, la taille ;

- le domicile ou la résidence ou, le cas échéant, la commune de rattachement de l'intéressé ou l'adresse de l'organisme d'accueil auprès duquel il est domicilié ;

- le cas échéant la décision attestant la capacité juridique du demandeur ;

b) Les informations relatives au titre :

- numéro de demande et de série fiscale du passeport ;

- type de passeport ;

- tarif du droit de timbre ;

- date et lieu de délivrance ;

- autorité de délivrance ;

- date d'expiration ;

- mention, avec la date, de la perte, du vol, de la destruction, de l'annulation ou du retrait ;

- mentions des justificatifs présentés à l'appui de la demande de passeport ;

- informations à caractère technique relatives à

l'établissement du titre ;

- informations relatives à la demande de passeport : numéro de demande, lieu de dépôt, date de réception de la demande, date de l'envoi du titre au guichet de dépôt, motif de non-délivrance ;

c) Les données relatives au fabricant du passeport et aux agents chargés de la délivrance du passeport :

- identifiant de l'agent qui enregistre la demande de passeport ;

- identifiant du fabricant du passeport ;

- références des agents mentionnés à l'article 20.

Article 20
Les destinataires des données à caractère personnel enregistrées dans le système de traitement automatisé prévu à l'article 18 et dans le composant électronique prévu à l'article 2 sont les fonctionnaires du ministère de l'intérieur spécialement affectés dans le service mettant en oeuvre ledit système, ainsi que les seuls agents et personnels spécialement affectés à l'instruction des demandes de délivrance des passeports, énumérés ci-après :

- les agents chargés de l'application de la réglementation relative au passeport au ministère de l'intérieur et au ministère des affaires étrangères, individuellement habilités par le ministre de l'intérieur ou le ministre des affaires étrangères ou par les fonctionnaires que ces ministres ont désignés à cet effet ;

- les agents des préfectures et des sous-préfectures chargés de la délivrance des titres visés aux articles 4 et 15, individuellement habilités par le préfet ou le sous-préfet ;

- les agents diplomatiques et consulaires chargés de la délivrance des titres visés aux articles 4 et 15, individuellement habilités par l'ambassadeur ou le consul ;

- les agents chargés de la délivrance des passeports de service au ministère de l'intérieur, individuellement habilités par le ministre de l'intérieur ou par les fonctionnaires désignés par le ministre à cet effet.

Article 21
Pour les besoins exclusifs de l'accomplissement de leurs missions, les personnels chargés des missions de recherche et de contrôle de l'identité des personnes, de vérification de la validité et de l'authenticité des passeports au sein des services de la police nationale, de la gendarmerie nationale et des douanes peuvent accéder aux données à caractère personnel contenues dans le composant électronique du passeport prévu à l'article 2 et enregistrées dans le système de traitement automatisé prévu à l'article 18.

Article 22
Pour l'instruction des demandes de passeport, il est vérifié, par la consultation du fichier des personnes recherchées, qu'aucune décision judiciaire ni aucune circonstance particulière ne s'oppose à sa délivrance.

Il est également procédé à une consultation du système de fabrication et de gestion informatisée des cartes nationales d'identité et du système de traitement automatisé prévu à l'article 18, afin de vérifier si des titres ont déjà été sollicités ou délivrés sous l'identité du demandeur.

Article 23
Le système de traitement automatisé prévu à l'article 18 fait l'objet d'une interconnexion avec les systèmes d'information Schengen et INTERPOL. Cette interconnexion porte sur les informations relatives aux numéros des passeports perdus ou volés ainsi que sur l'indication relative au pays émetteur, au type et au caractère vierge ou personnalisé du document.

Article 24
La durée de conservation des données à caractère personnel enregistrées dans le système de traitement automatisé prévu à l'article 18 est de quinze ans lorsque le titre est délivré à un majeur et de dix ans lorsqu'il est délivré à un mineur.

La durée de conservation de ces données à caractère personnel est de dix ans pour le passeport de service et le passeport de mission.

Article 25
La remise du passeport s'accompagne d'une copie sur papier des données nominatives enregistrées dans le composant électronique. Le titulaire exerce son droit de rectification pour ces données auprès de l'autorité de délivrance.

Article 26
Le droit d'accès et le droit de rectification s'exercent auprès de l'autorité de délivrance dans les conditions fixées aux articles 39 et 40 de la loi du 6 janvier 1978 susvisée.

Article 27
Le droit d'opposition prévu à l'article 38 de la loi du 6 janvier 1978 susvisée ne s'applique pas au présent traitement.

TITRE III : DISPOSITIONS FINALES ET TRANSITOIRES

Article 28
Un arrêté du ministre de l'intérieur fixe les dates à partir desquelles seront reçues les demandes de passeport électronique dans les départements en métropole.

Un arrêté conjoint du ministre de l'intérieur et du ministre de l'outre-mer fixe les dates à partir desquelles seront reçues les demandes de passeport électronique dans les départements d'outre-mer, les collectivités d'outre-mer et la Nouvelle-Calédonie.

Un arrêté conjoint du ministre de l'intérieur et du ministre des affaires étrangères fixe les dates à partir desquelles seront reçues les demandes de passeport électronique des Français établis hors de France.

Un arrêté du ministre de l'intérieur fixe la date à partir de laquelle seront reçues les demandes de passeport électronique de service.

Article 29
I. - Le présent décret est applicable à Mayotte, dans les îles Wallis et Futuna, en Polynésie française et en Nouvelle-Calédonie.

II. - Pour l'application du dernier alinéa de l'article 5, dans les collectivités d'outre-mer et en Nouvelle-Calédonie, les mots : « la loi » sont remplacés par les mots : « les dispositions applicables localement ».

III. - Pour son application à Mayotte, le mot : « préfet » est remplacé par les mots « représentant de l'Etat à Mayotte ».

Pour les demandeurs mineurs ayant conservé leur statut personnel, les mots : « exerçant l'autorité parentale » sont remplacés par les mots : « exerçant dans les faits l'autorité parentale ».

IV. - Pour son application dans les îles Wallis et Futuna, le mot : « commune » est remplacé par le mot : « circonscription territoriale ». Les mots : « préfet » et « sous-préfet » sont remplacés respectivement par les mots : « administrateur supérieur » et « délégué de l'administrateur supérieur ».

V. - Pour son application en Polynésie française, les mots : « préfet » et « sous-préfet » sont remplacés respectivement par les mots : « haut-commissaire de la République » et « chef de subdivision administrative ».

VI. - Pour son application en Nouvelle-Calédonie, les mots : « préfet » et « sous-préfet » sont remplacés respectivement par les mots : « haut-commissaire de la République » et « commissaire délégué ».

Article 30
Le décret n° 2001-185 du 26 février 2001 relatif aux conditions de délivrance et de renouvellement des passeports, le décret n° 2001-847 du 11 septembre 2001 relatif à la durée des passeports délivrés en Nouvelle-Calédonie, en Polynésie Française, dans les îles Wallis et Futuna, à Mayotte et à Saint-Pierre-et-Miquelon, à l'exception de son article 3, et le décret n° 2001-893 du 26 septembre 2001 relatif au passeport de service sont abrogés.

Toutefois, les autorités compétentes pourront délivrer des passeports en application des décrets mentionnés à l'alinéa précédent jusqu'aux dates fixées dans les conditions de l'article 28.

Article 31
Le ministre d'Etat, ministre de l'intérieur et de l'aménagement du territoire, le ministre des affaires étrangères, le ministre de l'économie, des finances et de l'industrie, le garde des sceaux, ministre de la justice, et le ministre de l'outre-mer sont chargés, chacun en ce qui le concerne, de l'exécution du présent décret, qui sera publié au Journal officiel de la République française.

Fait à Paris, le 30 décembre 2005.

Par Julien Le Clainche, Allocataire de recherche

Retrouver le décret n° 2005-1726 du 30 décembre 2005 relatif aux passeports électroniques sur **Legifrance**.

DROIT-TIC .com

R.D.T.I.C

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

DÉLIBÉRATIONS DE LA CNIL

DÉLIBÉRATION N° 2005-305 8 décembre 2005

PORTANT AUTORISATION UNIQUE DE TRAITEMENTS AUTOMATISÉS DE DONNÉES À CARACTÈRE PERSONNEL MIS EN ŒUVRE DANS LE CADRE DE DISPOSITIFS D'ALERTE PROFESSIONNELLE

Thèmes

Informatique et libertés, droit social, droit du travail

Abstract

Système d'alerte profesionnelle / whistleblowing, Sarbanes Oxley, finalité, identification, destinataire, transfert, conservation, information

Résumé

Délibération n° 2005-305 du 8 décembre 2005 portant autorisation unique de traitements automatisés de données à caractère personnel mis en œuvre dans le cadre de dispositifs d'alerte professionnelle

Délibération n° 2005-305 du 8 décembre 2005 portant autorisation unique de traitements automatisés de données à caractère personnel mis en œuvre dans le cadre de dispositifs d'alerte professionnelle

La Commission nationale de l'informatique et des libertés,

Vu la Convention n°108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

Vu 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 de données à caractère personnel et la libre circulation de ces données ;

Vu la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée par la loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, et notamment son article 25 I 4° et II ;

Vu le document d'orientation relatif aux dispositifs d'alerte professionnelle adopté par la Commission le 10 novembre 2005, annexé à la présente décision ;

Après avoir entendu M. Alex Türk, président, en son rapport, et Mme Pascale Compagnie, commissaire du Gouvernement, en ses observations,

Un dispositif d'alerte professionnelle est un système mis à la disposition des employés d'un organisme public ou privé pour les inciter, en complément des modes normaux d'alerte sur les dysfonctionnements de l'organisme, à signaler à leur employeur des comportements qu'ils estiment contraires aux règles applicables et pour organiser la vérification de l'alerte ainsi recueillie au sein de l'organisme concerné.

Constate que les dispositifs d'alerte professionnelle («whistleblowing») mis en œuvre sur les lieux de travail peuvent prendre la forme de traitements automatisés de données à caractère personnel susceptibles, du fait de leur portée, d'exclure des personnes du bénéfice de leur contrat de travail en l'absence de toute disposition législative ou réglementaire.

Dès lors, de tels dispositifs constituent des traitements relevant de l'article 25-I 4° de la loi du 6 janvier 1978 modifiée et doivent, à ce titre, être autorisés par la CNIL.

En vertu de l'article 25-II de la loi du 6 janvier 1978 modifiée, la Commission peut adopter une décision unique d'autorisation pour des traitements répondant notamment aux mêmes finalités, portant sur des catégories de données et des catégories de destinataires identiques.

Le responsable de traitement mettant en œuvre un dispositif d'alerte professionnelle dans le respect des dispositions de cette décision unique adresse à la Commission un engagement de conformité à la présente autorisation.

Décide que les responsables de traitement qui adressent à la Commission une déclaration comportant un engagement de conformité pour leurs traitements de données à caractère personnel répondant aux conditions fixées par la présente décision unique sont autorisés à mettre en œuvre ces traitements.

Article 1. Finalités du traitement

Seuls peuvent faire l'objet d'un engagement de conformité par référence à la présente décision unique les traitements mis en œuvre par les organismes publics ou privés dans le cadre d'un dispositif d'alerte professionnelle répondant à une obligation législative ou réglementaire de droit français visant à l'établissement de procédures de contrôle interne dans les domaines financier, comptable, bancaire et de la lutte contre la corruption.

Conformément à l'article 7-5° de la loi du 6 janvier 1978 modifiée, les traitements mis en œuvre dans les domaines comptable et d'audit par les entreprises concernées par la section 301(4) de la loi américaine dite «Sarbanes-Oxley» de juillet 2002 entrent également dans le champ de la présente décision.

Article 2. Traitement de l'identité de l'émetteur de l'alerte

L'émetteur de l'alerte professionnelle doit s'identifier mais son identité est traitée de façon confidentielle par l'organisation chargée de la gestion des alertes.

Cette organisation ne peut recueillir, par exception, l'alerte d'une personne qui souhaite rester anonyme qu'aux conditions suivantes :

- le traitement de cette alerte doit s'entourer de précautions particulières, telles qu'un examen préalable, par son premier destinataire, de l'opportunité de sa diffusion dans le cadre du dispositif,
- l'organisme n'incite pas les personnes ayant vocation à utiliser le dispositif à le faire de manière anonyme et la publicité faite sur l'existence du dispositif en tient compte. Au contraire, la procédure est conçue de façon à ce que les employés s'identifient auprès de l'organisation chargée de la gestion des alertes.

Article 3. Catégories de données à caractère personnel enregistrées

Seules les catégories de données suivantes peuvent être traitées :

- identité, fonctions et coordonnées de l'émetteur de l'alerte professionnelle ;
- identité, fonctions et coordonnées des personnes faisant l'objet d'une alerte ;
- identité, fonctions et coordonnées des personnes intervenant dans le recueil ou dans le traitement de l'alerte ;
- faits signalés ;
- éléments recueillis dans le cadre de la vérification des faits signalés ;
- compte rendu des opérations de vérification ;
- suites données à l'alerte.

Les faits recueillis sont strictement limités aux domaines concernés par le dispositif d'alerte. Des faits qui ne se rapportent pas à ces domaines peuvent toutefois être communiqués aux personnes compétentes de l'organisme concerné lorsque l'intérêt vital de cet organisme ou l'intégrité physique ou morale de ses employés est en jeu.

La prise en compte de l'alerte professionnelle ne s'appuie que sur des données formulées de manière objective, en rapport direct avec le champ du dispositif d'alerte et strictement nécessaires à la vérification des faits allégués. Les formulations utilisées pour décrire la nature des faits signalés font apparaître leur caractère présumé.

Article 4. Destinataires des données à caractère personnel

Les personnes spécialement chargées, au sein de l'organisme concerné, du recueil ou du traitement des alertes professionnelles ne sont destinataires de tout ou partie des données visées à l'article 3 que dans la mesure où ces données sont nécessaires à l'accomplissement de leurs missions.

Ces données peuvent être communiquées aux personnes spécialement chargées de la gestion des alertes professionnelles au sein du groupe de sociétés auquel appartient l'organisme concerné si cette communication est nécessaire à la vérification de l'alerte ou résulte de l'organisation du groupe.

S'il est fait recours à un prestataire de service pour recueillir ou traiter les alertes, les personnes spécialement chargées de ces missions au sein de l'organisme prestataire de service n'accèdent à tout ou partie des données visées à l'article 3 que dans la limite de leurs attributions respectives. Le prestataire de service éventuellement désigné pour gérer tout ou partie de ce dispositif s'engage notamment, par voie contractuelle, à ne pas utiliser les données à des fins détournées, à assurer leur confidentialité, à respecter la durée de conservation limitée des données et à procéder à la destruction ou à la restitution de tous les supports manuels ou informatisés de données à caractère personnel au terme de sa prestation.

Dans tous les cas, les personnes chargées du recueil et du traitement des alertes professionnelles sont en nombre limité, spécialement formées et astreintes à une obligation renforcée de confidentialité contractuellement définie.

Article 5. Transferts de données à caractère personnel hors de l'Union européenne

Le présent article s'applique dans les cas où les communications de données envisagées à l'article 4 concernent un transfert vers une personne morale établie dans un pays non membre de l'Union européenne n'accordant pas une protection suffisante au sens de l'article 68 de la loi du 6 janvier 1978 modifiée.

Dans ces cas, ces communications de données à caractère personnel doivent s'opérer conformément aux dispositions spécifiques de la loi du 6 janvier 1978 modifiée relatives aux transferts internationaux de données, et notamment son article 69, alinéa 8.

Il est satisfait à ces dispositions lorsque la personne morale au sein de laquelle travaille le destinataire des données a adhéré au Safe Harbor, dans la mesure où la société américaine concernée a expressément fait le choix d'inclure les données de ressources humaines dans le champ de cette adhésion.

Il est également satisfait à ces dispositions lorsque le destinataire a conclu un contrat de transfert basé sur les clauses contractuelles types émises par la Commission européenne dans ses décisions du 15 juin 2001 ou du 27 décembre 2004, ou lorsque le groupe auquel appartiennent les entités concernés ont adopté des règles internes dont la CNIL a préalablement reconnu qu'elles garantissent un niveau de protection suffisant de la vie privée et des droits fondamentaux des personnes. S'il est satisfait à ces conditions, et si le traitement dont le transfert est issu est par ailleurs conforme à l'ensemble des autres dispositions de la présente délibération, la présente délibération porte également autorisation du transfert envisagé en application de l'article 69, alinéa 8, de la loi du 6 janvier 1978 modifiée.

Article 6. Durée de conservation des données à caractère personnel

Les données relatives à une alerte considérée, dès son recueil par le responsable du traitement, comme n'entrant pas dans le champ du dispositif sont détruites ou archivées sans délai, sous réserve de l'application de l'avant-dernier alinéa de l'article 3.

Les données relatives à une alerte ayant fait l'objet d'une vérification sont détruites ou archivées par l'organisation chargée de la gestion des alertes dans un délai de deux mois à compter de la clôture des opérations de vérification lorsque l'alerte n'est pas suivie d'une procédure disciplinaire ou judiciaire.

Lorsqu'une procédure disciplinaire ou des poursuites judiciaires sont engagées à l'encontre de la personne mise en cause ou de l'auteur d'une alerte abusive, les données relatives à l'alerte sont conservées par l'organisation chargée de la gestion des alertes jusqu'au terme de la procédure.

Les données faisant l'objet de mesures d'archivage sont conservées, dans le cadre d'un système d'information distinct à accès restreint, pour une durée n'excédant pas les délais de procédures contentieuses.

Article 7. Mesures de sécurité

Le responsable des traitements prend toutes précautions utiles pour préserver la sécurité des données tant à l'occasion de leur recueil que de leur communication ou de leur conservation.

En particulier, les accès aux traitements de données s'effectuent par un identifiant et un mot de passe individuels, régulièrement renouvelés, ou par tout autre moyen d'authentification. Ces accès sont enregistrés et leur régularité est contrôlée.

L'identité de l'émetteur d'une alerte est traitée de façon confidentielle afin que celui-ci ne subisse aucun préjudice du fait de sa démarche.

Article 8. Information des utilisateurs potentiels du dispositif

Une information claire et complète des utilisateurs potentiels du dispositif d'alerte est réalisée.

Au delà de l'information collective et individuelle prévue par le Code du travail, et conformément à l'article 32 de la loi du 6 janvier 1978 modifiée, cette information précise notamment l'identification de l'entité responsable du dispositif, les objectifs poursuivis et les domaines concernés par les alertes, le caractère facultatif du dispositif, l'absence de conséquence à l'égard des employés de la non-utilisation de ce dispositif, les destinataires des alertes, les éventuels transferts de données à caractère personnel à destination d'un Etat non membre de la Communauté européenne, ainsi que l'existence d'un droit d'accès et de rectification au bénéfice des personnes identifiées dans le cadre de ce dispositif.

Il est clairement indiqué que l'utilisation abusive du dispositif peut exposer son auteur à des sanctions disciplinaires ainsi qu'à des poursuites judiciaires mais qu'à l'inverse, l'utilisation de bonne foi du dispositif, même si les faits s'avèrent par la suite inexacts ou ne donnent lieu à aucune suite, n'exposera son auteur à aucune sanction disciplinaire.

Article 9. Information de la personne faisant l'objet d'une alerte professionnelle

La personne qui fait l'objet d'une alerte est, conformément aux articles 6 et 32 de loi du 6 janvier 1978, informée par le responsable du dispositif dès l'enregistrement, informatisé ou non, de données la concernant afin de lui permettre de s'opposer au traitement de ces données.

Lorsque des mesures conservatoires sont nécessaires, notamment pour prévenir la destruction de preuves relatives à l'alerte, l'information de cette personne intervient après l'adoption de ces mesures.

Cette information, qui est réalisée selon des modalités permettant de s'assurer de sa bonne délivrance à la personne concernée, précise notamment l'entité responsable du dispositif, les faits qui sont reprochés, les services éventuellement destinataires de l'alerte ainsi que les modalités d'exercice de ses droits d'accès et de rectification. Si elle n'en a pas bénéficié auparavant, la personne reçoit également une information conforme à l'article 8 de la présente décision.

Article 10. Respect des droits d'accès et de rectification

Conformément aux articles 39 et 40 de la loi du 6 janvier 1978 modifiée, le responsable du dispositif d'alerte garantit à toute personne identifiée dans le dispositif d'alerte professionnelle le droit d'accéder aux données la concernant et d'en demander, si elles sont inexactes, incomplètes, équivoques ou périmées, la rectification ou la suppression.

La personne qui fait l'objet d'une alerte ne peut en aucun cas obtenir communication du responsable du traitement, sur le fondement de son droit d'accès, des informations concernant l'identité de l'émetteur de l'alerte.

Article 11

Tout dispositif d'alerte professionnelle prévoyant la mise en œuvre de traitement de données à caractère personnel ne répondant pas aux dispositions précédentes doit faire l'objet d'une demande d'autorisation auprès de la Commission dans les formes prescrites par les articles 25-I 4° et 30 de la loi du 6 janvier 1978 modifiée.

Article 12

La présente délibération sera publiée au Journal officiel de la République française.

Le président Alex Türk

ANNEXE

Document d'orientation adopté par la Commission le 10 novembre 2005 pour la mise en œuvre de dispositifs d'alerte professionnelle conformes à la loi du 6 janvier 1978 modifiée en août 2004, relative à l'informatique, aux fichiers et aux libertés

La Commission nationale de l'informatique et des libertés constate le développement récent en France de dispositifs permettant à des employés de signaler le comportement de leurs collègues de travail supposé contraire à la loi ou aux règles établies par l'entreprise.

Ces dispositifs «d'alerte professionnelle» («whistleblowing») ne sont ni prévus, ni interdits par le code du travail. Quand ils s'appuient sur le traitement de données à caractère personnel c'est-à-dire la collecte, l'enregistrement, la conservation et la diffusion d'informations relatives à une personne physique identifiée ou identifiable, ils sont soumis à la loi du 6 janvier 1978 modifiée, que le traitement soit réalisé sur support informatique ou sur support papier. Lorsqu'ils sont automatisés, ils doivent faire l'objet d'une autorisation de la CNIL, en application de l'article 25-4° de cette loi du fait qu'ils sont susceptibles d'exclure des personnes du bénéfice d'un droit ou de leur contrat de travail en l'absence de toute disposition législative ou réglementaire spécifique.

La CNIL a refusé en mai 2005 d'autoriser deux systèmes spécifiques de «lignes éthiques» relevant de cette démarche d'alerte professionnelle. Pour autant elle n'a pas d'opposition de principe à de tels dispositifs dès lors

que les droits des personnes mises en cause directement ou indirectement dans une alerte sont garantis au regard des règles relatives à la protection des données personnelles. En effet, ces personnes, en plus des droits de la défense qui leur sont assurés par la législation du travail en cas d'engagement d'une procédure disciplinaire, disposent de droits particuliers qui leur sont reconnus par la loi «informatique et libertés» ou la directive européenne 95/46/CE du 24 octobre 1995 quand des informations les concernant font l'objet d'un traitement : droit à ce que ces informations soient recueillies de manière loyale, droit à être informé du traitement de ces informations, droit de s'opposer à ce traitement si un motif légitime peut être invoqué, droit de rectifier ou de faire supprimer les informations inexactes, incomplètes, équivoques ou périmées.

Afin de contribuer à la mise en œuvre de dispositifs d'alerte respectueux des principes définis par la loi et la directive, la CNIL préconise l'adoption par les entreprises des règles suivantes qui ne portent que sur l'application de ces textes, à l'exclusion des questions pour lesquelles la CNIL n'a pas de compétence, en particulier celles relatives à la législation du travail.

1) Portée du dispositif d'alerte : un caractère complémentaire, un champ restreint, un usage facultatif

Le fonctionnement normal d'une organisation implique que les alertes relatives à un dysfonctionnement, dans quelque domaine que ce soit, remontent jusqu'aux dirigeants par la voie hiérarchique ou par des modes ouverts d'alerte tels que l'intervention des représentants du personnel ou, en matière de contrôle des comptes, les rapports des commissaires aux comptes. Dans la législation française, la protection et l'indépendance des uns et des autres sont du reste particulièrement assurées.

La mise en place d'un dispositif d'alerte peut être justifiée par l'hypothèse que ces canaux d'information pourraient ne pas fonctionner dans certaines circonstances. Toutefois, un tel dispositif ne saurait être conçu, par les entreprises, comme un mode normal de signalement des dysfonctionnements de l'entreprise, à part égale avec les modes de signalement gérés par des personnes dont les fonctions ou les attributions consistent précisément à repérer et traiter de tels dysfonctionnements. En ce sens, les dispositifs d'alerte doivent être conçus comme uniquement complémentaires par rapport aux autres modes d'alerte dans l'entreprise.

Afin de tenir compte de ce caractère intrinsèquement complémentaire, un dispositif d'alerte doit être limité dans son champ. Les dispositifs à portée générale et indifférenciée (tels que ceux destinés à garantir à la fois le respect des règles légales, du règlement intérieur et des règles internes de conduite professionnelle) soulèvent en effet une difficulté de principe au regard de la loi « informatique et libertés » eu égard aux risques de mise en cause abusive ou disproportionnée de l'intégrité professionnelle voire personnelle des employés concernés.

A cet égard, il résulte de l'article 7 de la loi du 6 janvier 1978 modifiée que les dispositifs d'alerte ne peuvent être considérés comme légitimes que du fait de l'existence d'une obligation légale (législative ou réglementaire) imposant la mise en place de tels dispositifs (article 7-1°), ou du fait de l'intérêt légitime du responsable de traitement, dès lors que celui-ci est établi, et « *sous réserve de ne pas méconnaître l'intérêt ou les droits et libertés fondamentaux de la personne concernée* » (article 7-5°).

Cette légitimité est acquise en vertu de l'article 7-1° de la loi du 6 janvier 1978 quand des dispositifs d'alerte sont mis en œuvre à seule fin de répondre à une obligation législative ou réglementaire de droit français visant à l'établissement de procédures de contrôle interne dans des domaines précisément définis. Une telle obligation résulte clairement, par exemple, des dispositions relatives au contrôle interne des établissements de crédit et des entreprises d'investissement (arrêté du 31 mars 2005 modifiant le règlement du Comité de la réglementation bancaire et financière n°97-02 du 21 février 1997).

En revanche, il ne semble pas que le simple fait de l'existence d'une disposition légale étrangère en vertu de laquelle un dispositif d'alerte serait mis en place permette de légitimer un traitement de données personnelles au sens de l'article 7-1°. Tel est le cas des dispositions de la Section 301(4) de la loi Sarbanes-Oxley qui prévoient que les employés d'une entreprise doivent pouvoir faire état au comité d'audit de leurs inquiétudes quant à une comptabilité ou un audit douteux en étant assurés de bénéficier de garanties de confidentialité et d'anonymat.

Il est cependant impossible, dans ce cas, d'ignorer l'intérêt légitime, au sens de l'article 7-5° de la loi du 6 janvier 1978, que les sociétés françaises cotées aux Etats-Unis ou les sociétés françaises filiales de sociétés cotées aux Etats-Unis, tenues de certifier leurs comptes auprès des autorités boursières américaines, ont à mettre en place des procédures d'alerte quant à des dysfonctionnements supposés en matière comptable et de contrôle des comptes. A l'évidence, la remontée jusqu'au conseil d'administration d'informations relatives, par exemple, à des suspicions de manipulations comptables pouvant avoir un impact sur les résultats financiers de l'entreprise est une préoccupation essentielle pour les entreprises faisant appel public à l'épargne.

Loin de se limiter aux Etats-Unis, des initiatives en la matière ont également été prises en Europe (cf.

notamment la récente recommandation de la Commission européenne du 15 février 2005 concernant le rôle des administrateurs non exécutifs et des membres de conseil de surveillance des sociétés cotées et les comités du conseil d'administration et de surveillance), qui poursuivent le même objectif de renforcement de la sécurité des marchés financiers que la loi Sarbanes-Oxley. Ces différents textes caractérisent manifestement, au sens de l'article 7-5° de la loi du 6 janvier 1978, l'intérêt légitime de l'entreprise à mettre en place des dispositifs d'alerte dans les domaines qu'ils couvrent, et, dans ce contexte, ceux-ci doivent donc être considérés comme acceptables.

Pour les mêmes raisons, sont légitimes les dispositifs d'alerte qui visent à lutter contre la corruption, par exemple celle d'agents publics étrangers dans les transactions commerciales internationales (convention OCDE du 17 décembre 1997, ratifiée par la loi n°99-424 du 27 mai 1999). Les dispositifs d'alerte limités au champ ainsi défini bénéficieront d'une autorisation unique de la CNIL, sous réserve du respect des autres règles recommandées par elle. En revanche, pour les dispositifs ne se fondant pas sur des obligations législatives ou réglementaires de contrôle interne dans les domaines financier, comptable, bancaire et de la lutte contre la corruption, la CNIL conduira une analyse au cas par cas, dans le cadre de ses pouvoirs d'autorisation, de la légitimité des finalités poursuivies et de la proportionnalité du dispositif d'alerte envisagé.

Afin de prévenir un usage détourné du dispositif d'alerte pour dénoncer des faits sans rapport avec les domaines définis a priori, le responsable de ce dispositif doit clairement indiquer qu'il est strictement réservé à de tels domaines et doit s'interdire d'exploiter les alertes qui y sont étrangères, sauf si l'intérêt vital de l'entreprise, l'intégrité physique ou morale de ses employés est en jeu.

Plus généralement, l'utilisation par les personnels d'un dispositif d'alerte légitimement mis en œuvre ne peut revêtir qu'un caractère non obligatoire. En ce sens, le ministère de l'emploi, du travail et de l'insertion professionnelle des jeunes a souligné, dans une lettre adressée à la CNIL, que « l'utilisation des dispositifs d'alerte ne doit pas faire l'objet d'une obligation mais d'une simple incitation. (…) Rendre obligatoire la dénonciation revient donc en réalité à transférer sur les salariés la charge de l'employeur en matière de respect du règlement intérieur. On peut également estimer que l'obligation de dénonciation serait contraire à l'article L120-2 du code du travail en tant que sujétion non proportionnée à l'objectif à atteindre ».

2) Une définition des catégories de personnes concernées par le dispositif d'alerte

Conformément au principe de proportionnalité, les catégories de personnels

susceptibles de faire l'objet d'une alerte devraient être précisément

définies en référence aux motifs légitimant la mise en œuvre du dispositif

d'alerte.

Cette définition relève de la compétence du chef d'entreprise à qui il

appartient, dans le respect des procédures prévues en droit du travail, de

fixer les limites de la procédure.

3) Un traitement restrictif des alertes anonymes

La possibilité de réaliser une alerte de façon anonyme ne peut que

renforcer le risque de dénonciation calomnieuse. A l'inverse,

l'identification de l'émetteur de l'alerte ne peut que contribuer à

responsabiliser les utilisateurs du dispositif et ainsi à limiter un tel

risque. En effet, l'alerte identifiée présente plusieurs avantages et

- d'éviter des dérapages vers la délation et la dénonciation calomnieuse ;
- d'organiser la protection de l'auteur de l'alerte contre d'éventuelles représailles ;
- d'assurer un meilleur traitement de l'alerte en ouvrant la possibilité de demander à son auteur des précisions complémentaires.

La protection de l'émetteur de l'alerte est une exigence consubstantielle à un dispositif d'alerte. La CNIL n'a pas à se prononcer sur les moyens de l'assurer sauf sur un point qui résulte clairement de la loi «informatique et libertés» : l'identité de l'émetteur doit être traitée de façon confidentielle afin que celui ne subisse aucun préjudice du fait de sa démarche. En particulier, cette identité ne peut être communiquée à la personne mise en cause sur le fondement du droit d'accès prévu par l'article 39 de cette loi.

Cependant, l'existence d'alertes anonymes, même et surtout en l'absence de systèmes organisés d'alerte confidentielle, est une réalité. Il est également difficile pour les responsables d'une organisation d'ignorer ce type d'alerte, quand bien même ils n'y seraient pas favorables par principe.

Le traitement de telles alertes doit s'entourer de précautions particulières, notamment un examen préalable, par leur premier destinataire, de l'opportunité de leur diffusion dans le cadre du dispositif. En tout état de cause, l'organisation ne doit pas inciter les personnes ayant vocation à utiliser le dispositif à le faire de manière anonyme et la publicité faite sur l'existence du dispositif doit en tenir compte. Au contraire, la procédure doit être conçue de manière à ce que les employés s'identifient à chaque communication d'informations par la procédure d'alerte et soumettent des informations relatives à des faits plutôt qu'à des personnes.

4) La diffusion d'une information claire et complète sur le dispositif d'alerte

Une information claire et complète des utilisateurs potentiels du dispositif d'alerte doit être réalisée par tout moyen approprié. Au delà de l'information collective et individuelle prévue par le code du travail, et conformément à l'article 32 de la loi du 6 janvier 1978 modifiée, cette information doit notamment préciser l'identification de l'entité responsable du dispositif, les objectifs poursuivis et le domaine concerné par les alertes, le caractère facultatif du dispositif, l'absence de conséquence à l'égard des employés de la non-utilisation de ce dispositif, les destinataires des alertes, ainsi que l'existence d'un droit d'accès et de rectification au bénéfice des personnes identifiées dans le cadre de ce dispositif.

Il doit enfin être clairement indiqué que l'utilisation abusive du dispositif peut exposer son auteur à des sanctions disciplinaires ainsi qu'à des poursuites judiciaires, mais qu'à l'inverse, l'utilisation de bonne foi du dispositif, même si les faits s'avèrent par la suite inexacts ou ne donnent lieu à aucune suite, ne peut exposer son auteur à des sanctions.

5) Un recueil des alertes par des moyens dédiés

Le recueil des alertes peut reposer sur tous moyens, informatisés ou non, de traitement des données.

Ces moyens doivent être dédiés au dispositif d'alerte afin d'écarter tout risque de détournement de finalité et de renforcer la confidentialité des données.

6) Des données d'alerte pertinentes, adéquates et non excessives

Le support permettant la prise en compte de l'alerte professionnelle ne doit comporter que des données formulées de manière objective, en rapport direct avec le champ du dispositif d'alerte et strictement nécessaires à la vérification des faits allégués.

Les formulations utilisées pour décrire la nature des faits signalés doivent faire apparaître leur caractère présumé.

7) Une gestion interne des alertes réservée à des spécialistes, dans un cadre confidentiel

Le recueil et le traitement des alertes professionnelles doivent être confiés à une organisation spécifique mise en place au sein de l'entreprise concernée pour traiter ces questions. Les personnes chargées de traiter les alertes doivent être en nombre limité, spécialement formées et astreintes à une obligation renforcée de confidentialité contractuellement définie.

La confidentialité des données à caractère personnel doit être garantie tant à l'occasion de leur recueil que de leur communication ou de leur conservation.

Les données recueillies par le dispositif d'alerte peuvent être communiquées au sein du groupe si cette communication est nécessaire aux besoins de l'enquête et résulte de l'organisation du groupe. Une telle communication sera considérée comme nécessaire aux besoins de l'enquête par exemple si l'alerte met en cause un collaborateur d'une autre personne morale du groupe, un membre de haut niveau ou un organe de direction de l'entreprise concernée. Dans ce cas, les données ne doivent être transmises, dans un cadre confidentiel et sécurisé, qu'à l'organisation compétente de la personne morale destinataire apportant des garanties équivalentes dans la gestion des alertes professionnelles.

Si une telle communication s'avère nécessaire, et ce vers une personne morale établie dans un pays non membre de l'Union européenne n'accordant pas une protection adéquate au sens de la directive 95/46/CE du 24 octobre 1995, il doit être fait application des dispositions spécifiques de la loi du 6 janvier 1978 modifiée relatives aux transferts internationaux de données (encadrement juridique particulier et information des personnes concernées sur le fait que les données seront transférées vers un tel pays).

Enfin, dans l'hypothèse où il serait envisagé d'avoir recours à un prestataire pour gérer le dispositif d'alerte, celui-ci doit s'engager contractuellement à ne pas utiliser les données à des fins détournées, à assurer leur confidentialité, et à respecter la durée de conservation limitée des données. L'entreprise concernée restera en tout état de cause responsable des traitements que le prestataire effectuera pour son compte.

8) La possibilité de rapports d'évaluation du dispositif

Dans le cadre de l'évaluation du dispositif d'alerte professionnelle, l'entreprise responsable peut communiquer aux entités chargées de cette mission au sein de son groupe toutes les informations statistiques utiles à leur mission (telles que les données relatives aux typologies d'alertes reçues et aux mesures correctives prises).

Ces informations ne doivent en aucun cas permettre l'identification directe ou indirecte des personnes concernées par les alertes.

9) Une conservation limitée des données à caractère personnel

Les données relatives à une alerte jugée infondée par l'entité responsable des alertes doivent être détruites sans délai.

Les données relatives aux alertes ayant nécessité une vérification ne doivent pas être conservées au delà de deux mois à compter de la clôture des opérations de vérification, sauf engagement d'une procédure disciplinaire ou de poursuites judiciaires à l'encontre de la personne mise en cause ou de l'auteur d'une alerte abusive.

10) Une information précise de la personne mise en cause

Conformément aux articles 6 et 32 de loi du 6 janvier 1978 modifiée l'information de la personne identifiée visée par une alerte doit être par principe réalisée par le responsable du dispositif dès l'enregistrement, informatisé ou non, des données la concernant afin de lui permettre de s'opposer sans délai au traitement de ces données.

Toutefois, l'information de la personne mise en cause ne saurait intervenir avant l'adoption de mesures conservatoires lorsque celles-ci s'avèrent indispensables, notamment pour prévenir la destruction de preuves nécessaires au traitement de l'alerte.

Cette information est réalisée selon des modalités permettant de s'assurer de sa bonne délivrance à la personne concernée.

Elle doit notamment préciser au salarié mis en cause l'entité responsable du dispositif, les faits qui lui sont reprochés, les services éventuellement destinataires de l'alerte ainsi que les modalités d'exercice de ses droits d'accès et de rectification.

11) Le respect des droits d'accès et de rectification

Conformément aux articles 39 et 40 de la loi du 6 janvier 1978 modifiée toute personne identifiée dans le dispositif d'alerte professionnelle peut accéder aux données la concernant et en demander, le cas échéant, la rectification ou la suppression.

Elle ne peut en aucun cas obtenir communication, sur le fondement de son droit d'accès, des informations concernant des tiers, telles que l'identité de l'émetteur de l'alerte.

Pour pus d'informations, consultez le dossier "Travail" édité par la CNIL

Référence : C.N.I.L, délibération du 08 décembre 2005, *N° 2005-305 PORTANT AUTORISATION UNIQUE DE TRAITEMENTS AUTOMATISÉS DE DONNÉES À CARACTÈRE PERSONNEL MIS EN ŒUVRE DANS LE CADRE DE DISPOSITIFS D'ALERTE PROFESSIONNELLE*, DROIT-TIC
http://www.droit-tic.com/juris/aff.php?id_juris=61

DROIT-TIC.com

R.D.T.I.C

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

DÉLIBÉRATION

N° 2005-285

22 novembre 2005

portant recommandation sur la mise en œuvre par des particuliers de sites web diffusant ou collectant des données à caractère personnel dans le cadre d'une activité exclusivement personnelle

Thèmes
Informatique et libertés, Loi applicable et juridiction compétente

Abstract
Site personnel, conditions de licéité, consentement (oui), information (oui), droit accès rectification opposition (oui), données relatives aux infractions, condamnations et mesures de sûreté (non), données sensibles (non), proportionnalité
Résumé

La CNIL précise les conditions de licéité de la mise en œuvre par des particuliers de sites web diffusant ou collectant des données à caractère personnel dans le cadre d'une activité exclusivement personnelle

J.O n° 293 du 17 décembre 2005
texte n° 80

Commission nationale de l'informatique et des libertés

Délibération n° 2005-285 du 22 novembre 2005 portant recommandation sur la mise en oeuvre par des particuliers de sites web diffusant ou collectant des données à caractère personnel dans le cadre d'une activité exclusivement personnelle

NOR: CNIX0508884X

La Commission nationale de l'informatique et des libertés,

Vu la convention n° 108 du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

Vu 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 ;

Vu la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel ;

Vu la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique ;

Vu la loi du 29 juillet 1881 sur la liberté de la presse ;

Vu l'article 9 du code civil ;

Vu la délibération de la Commission nationale de l'informatique et des libertés n° 2005-284 du 22 novembre 2005 décidant la dispense de déclaration des sites web diffusant ou collectant des données à caractère personnel mis en oeuvre par des particuliers dans le cadre d'une activité exclusivement personnelle ;

Après avoir entendu M. Emmanuel de Givry, commissaire, en son rapport et Mme Pascale Compagnie, commissaire du Gouvernement, en ses observations,

Formule les observations suivantes :

La commission constate le développement de l'utilisation par les particuliers, à titre privé, de sites web comme moyen de communication.

La commission relève que le développement des sites web personnels participe d'une utilisation nouvelle de l'internet par les particuliers et s'inscrit dans le cadre de la liberté d'expression.

Ces sites peuvent ainsi avoir pour vocation la diffusion d'informations à destination du cercle familial ou des proches, la mise en ligne d'un journal personnel (blocs-notes ou « blogs ») ou la présentation de sujets d'intérêt personnel (loisirs, sport, culture, diffusion d'idées, etc.).

Ils peuvent être créés directement par les particuliers eux-mêmes ou hébergés et maintenus par des prestataires de service.

Le traitement et la diffusion d'informations à partir d'un site web sont soumis notamment aux dispositions de la loi du 21 juin 2004 pour la confiance dans l'économie numérique, de la loi du 29 juillet 1881 sur la liberté de la presse et de la loi « informatique et libertés » du 6 janvier 1978 modifiée.

Les sites mis en oeuvre par des particuliers sont susceptibles de permettre, d'une part, la collecte de données à caractère personnel se rapportant aux personnes qui s'y connectent et, d'autre part, la diffusion de données à caractère personnel (nom, images de personnes ou tout autre élément permettant d'identifier une personne physique).

La diffusion ou la collecte d'une donnée à caractère personnel à partir d'un site web constitue un traitement automatisé de données à caractère personnel soumis aux dispositions de la loi « informatique et libertés » du 6 janvier 1978 modifiée.

Le responsable du traitement ainsi mis en oeuvre est, au regard de l'article 3 de la loi « informatique et libertés », la personne qui prend l'initiative de la création du site, que la gestion technique de celui-ci soit le fait de la personne elle-même ou d'un prestataire de service.

Faisant application de l'article 24 de la loi, la commission a décidé de dispenser de déclaration les sites mis en oeuvre par des particuliers dans le cadre d'une activité privée diffusant ou collectant des données à caractère personnel (délibération n° 2005-284 du 22 novembre 2005).

Pour autant, la CNIL estime utile de préciser les règles applicables à la mise en oeuvre de sites web personnels lorsque ceux-ci collectent ou diffusent des données à caractère personnel,

Recommande :
En ce qui concerne la diffusion au public, à partir d'un site web, de données à caractère personnel :

La commission rappelle que la diffusion de données à caractère personnel (nom, photographie, etc.) est soumise au consentement préalable des personnes auxquelles elles se rapportent. La diffusion de données à caractère personnel relatives à des mineurs, et notamment leur image, ne peut s'effectuer qu'avec leur accord et l'autorisation expresse des parents ou du responsable légal.

Les personnes dont les données sont susceptibles d'être diffusées doivent avoir été préalablement informées :

- de l'identité du responsable du traitement, à savoir de la personne souhaitant procéder à la diffusion ;

- de la finalité poursuivie, à savoir de leur diffusion sur internet, des conséquences d'une telle diffusion et de l'objet du site procédant à cette diffusion ;

- de l'existence d'un droit d'accès, de rectification et d'opposition.

Cette information n'est pas requise lorsque les données concernées ont été rendues publiques par la personne concernée.

Les personnes dont les données à caractère personnel sont traitées peuvent s'opposer à tout moment à la diffusion des données les concernant.

Les sites web personnels ne peuvent diffuser des données à caractère personnel relatives aux infractions, condamnations et mesures de sûreté concernant des tiers.

Au regard des risques de captation et de réutilisation des données qui sont diffusées sur le réseau internet, la commission recommande que les données qui font apparaître, directement ou indirectement, les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes, ou qui sont relatives à la santé ou à la vie sexuelle ne soient pas diffusées à partir d'un site web personnel.

Lorsque les sites ont vocation à n'être consultés que par un nombre limité de personnes (sites exclusivement destinés au cercle familial ou aux proches), la commission recommande que les données diffusées ne soient accessibles qu'aux seules personnes identifiées par le responsable du site web.

En ce qui concerne la collecte de données à caractère personnel à partir d'un site web :

Les sites web mis en oeuvre par des particuliers peuvent conduire ceux-ci à recueillir des informations sur les personnes qui s'y connectent (nom, adresse électronique, etc.).

La commission rappelle que les personnes auprès desquelles sont recueillies ces informations doivent être informées de la finalité de cette collecte, des destinataires ou catégories de destinataires des données et de l'existence d'un droit d'accès, de rectification et d'opposition.

Les données collectées ne peuvent être conservées que pour une durée limitée, en relation avec l'objet du site.

La transmission à des tiers, par le responsable du site, des données collectées ne peut s'effectuer que dans le cadre d'activités privées, après que la personne concernée en a été informée et a été mise en mesure de s'y opposer.

La présente délibération sera publiée au Journal officiel de la République française.

Pour la commission :

Le président,

A. Türk

La délibération sur Legifrance
<http://www.legifrance.gouv.fr/WAspad/UnTexteDeJorf?numjo=CNIX0508884X>

Référence : C.N.I.L, délibération du 22 novembre 2005, *N° 2005-285 PORTANT RECOMMANDATION SUR LA MISE EN OEUVRE PAR DES PARTICULIERS DE SITES WEB DIFFUSANT OU COLLECTANT DES DONNÉES À CARACTÈRE PERSONNEL DANS LE CADRE D'UNE ACTIVITÉ EXCLUSIVEMENT PERSONNELLE*, DROIT-TIC
http://www.droit-tic.com/juris/aff.php?id_juris=58

DROIT-TIC.com

R.D.T.I.C

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

DÉLIBÉRATION

N° 2005-284

22 novembre 2005

Décidant la dispense de déclaration des sites web diffusant ou collectant des données à caractère personnel mis en œuvre par des particuliers dans le cadre d'une activité exclusivement personnelle (norme d'exonération n° 6)

Thèmes
Informatique et libertés, Loi applicable et juridiction compétente

Abstract
CNIL, procédure, formalités préalables, sites web mis en oeuvre par des particuliers dans le cadre d'une activité exclusivement personnelle, dispense (oui)

Résumé
par le biais de la norme d'exonération n° 6, la CNIL décide de dispenser de déclaration les sites web diffusant ou collectant des données à caractère personnel mis en oeuvre par des particuliers dans le cadre d'une activité exclusivement personnelle

J.O n° 293 du 17 décembre 2005
texte n° 79

Commission nationale de l'informatique et des libertés

Délibération n° 2005-284 du 22 novembre 2005 décidant la dispense de déclaration des sites web diffusant ou collectant des données à caractère personnel mis en oeuvre par des particuliers dans le cadre d'une activité exclusivement personnelle (norme d'exonération n° 6)

NOR: CNIX0508883X

La Commission nationale de l'informatique et des libertés,

Vu la convention n° 108 du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

Vu 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 ;

Vu la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel ;

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

Après avoir entendu M. Emmanuel de Givry, commissaire, en son rapport et Mme Pascale Compagnie, commissaire du Gouvernement, en ses observations ;

La commission constate le développement de l'utilisation par les particuliers, à titre privé, de sites web comme moyen de communication, notamment au travers des blocs-notes ou « blogs » ;

Ces sites sont susceptibles de permettre, d'une part, la collecte de données à caractère personnel de personnes qui s'y connectent et, d'autre part, la diffusion de données à caractère personnel (nom, images de personnes ou tout autre élément permettant d'identifier une personne physique) ;

La diffusion ou la collecte d'une donnée à caractère personnel à partir d'un site web constitue un traitement

automatisé de données à caractère personnel soumis aux dispositions de la loi du 6 janvier 1978 modifiée, notamment celles relatives aux formalités préalables,

Décide :
De faire application des dispositions de l'article 24-II de la loi du 6 janvier 1978 modifiée et de dispenser de déclaration les sites web diffusant ou collectant des données à caractère personnel mis en oeuvre par des particuliers dans le cadre d'une activité exclusivement personnelle.

Par opposition, la diffusion et la collecte de données à caractère personnel opérée à partir d'un site web dans le cadre d'activités professionnelles, politiques, ou associatives restent soumises à l'accomplissement des formalités préalables prévues par la loi.

La dispense de déclaration n'exonère pas le responsable de tels traitements des obligations prévues par les textes applicables à la protection des données à caractère personnel.

La présente délibération sera publiée au Journal officiel de la République française.

Pour la commission :

Le président,

A. Türk

La délibération sur Legifrance
<http://www.legifrance.gouv.fr/WAspad/UnTexteDeJorf?numjo=CNIX0508883X>

Référence :

C.N.I.L, délibération du 22 novembre 2005, *N° 2005-284 DÉCIDANT LA DISPENSE DE DÉCLARATION DES SITES WEB DIFFUSANT OU COLLECTANT DES DONNÉES À CARACTÈRE PERSONNEL MIS EN OEUVRE PAR DES PARTICULIERS DANS LE CADRE D'UNE ACTIVITÉ EXCLUSIVEMENT PERSONNELLE (NORME D'EXONÉRATION N° 6)*, DROIT-TIC
http://www.droit-tic.com/juris/aff.php?id_juris=57

DROIT-TIC .com

R.D.T.I.C

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

DÉLIBÉRATION N° 2005-049 24 mars 2005

Relative à l'adoption du décret d'application de la loi n° 2004-801

Thèmes
Informatique et libertés, Droits de la personnalité

Résumé
Avis de la CNIL relatif au projet de décret en Conseil d'Etat, pris pour l'application de la loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données et modifiant la loi n° 78/17

Délibération n°2005-049 du 24 mars 2005 relative à l'adoption du décret d'application de la loi n° 2004-801

Saisie par le ministre de la justice d'un projet de décret en Conseil d'Etat, pris pour l'application de la loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ;

Vu la Convention n° 108 du 28 janvier 1981 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

Vu 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 ;

Vu la loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ;

Après avoir entendu M. Alex Türk, président, en son rapport et Mme Charlotte-Marie Pitrat, commissaire du Gouvernement, en ses observations ;

Emet l'avis suivant :

La Commission nationale de l'informatique et des libertés a été saisie, le 10 mars 2005, par le ministre de la justice, du décret pris pour l'application de la loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. L'article 71 de ce dernier texte prévoit en effet la consultation de la CNIL préalablement à l'examen en Conseil d'Etat.

En préambule, la Commission observe que le projet de décret, encore incomplet, qui lui est soumis comporte 78 articles et entre dans le détail de l'organisation, du fonctionnement et des procédures de la CNIL. Or l'article 13 de la loi du 6 janvier 1978 modifiée dispose dans son dernier alinéa que « La commission établit un règlement intérieur. Ce règlement fixe les règles relatives à l'organisation et au fonctionnement de la commission. Il précise notamment les règles relatives aux délibérations, à l'instruction des dossiers et à leur présentation devant la commission. » alors que l'article 8 de la loi de 1978 dans sa version antérieure à la loi du 6 août 2004 se bornait à dire que la Commission établit « son règlement intérieur ».

Certes l'article 71 de la loi du 6 janvier 1978 modifiée prévoit que « des décrets en Conseil d'État, pris après avis de la Commission nationale de l'informatique et des libertés, fixent les modalités d'application de la présente loi. » Il semble néanmoins à la Commission que les termes de l'article 13 auraient pu conduire à limiter plus étroitement l'intervention du pouvoir règlementaire dans des matières que le législateur a expressément renvoyées au règlement intérieur de la CNIL. Toutefois, à ce stade du processus d'élaboration du décret et compte tenu du fait que les services de la CNIL ont été étroitement associés par le ministère de la justice à la rédaction du texte soumis à la concertation interministérielle, la Commission laisse à cette observation un caractère général et ne propose pas de modifications qui en soient la traduction.

Elle demande en revanche que les modifications présentées sous forme d'amendements dans la suite de la présente délibération soient apportées au texte qui lui a été soumis.

Chapitre Ier : Organisation et fonctionnement de la Commission Article 2 Règles de quorum

Dans le dernier alinéa de cet article, substituer aux mots « à l'alinéa précédent » les mots « aux alinéas précédents »

Exposé des motifs

Amendement rédactionnel

Article 4 Rattachement au budget du ministère de la justice

Rédiger ainsi le premier alinéa de cet article

« Les crédits nécessaires au fonctionnement de la commission sont inscrits au budget du ministère de la justice dans des conditions qui garantissent l'autonomie de la commission et qui font l'objet d'une convention avec ce ministère. »

Exposé des motifs

Cet amendement tire d'abord les conséquences de la disparition de la notion de chapitre budgétaire puisqu'en fait l'individualisation des crédits de la CNIL se fait désormais dans une action au sein d'un programme du ministère de la justice.

En second lieu il pose le principe du maintien de l'autonomie actuelle de gestion de la CNIL par rapport au responsable du programme auquel elle est rattachée, conformément aux engagement qui ont été donnés au président de la CNIL lors de la définition de la nouvelle architecture du budget de l'Etat. Cette autonomie pourrait être formalisée dans une convention entre la CNIL et le ministère de la justice.

Titre II : Des formalités préalables à la mise en œuvre des traitements de données à caractère personnel Chapitre Ier : Dispositions générales Article 7 Modalités d'envoi et de réception des dossiers de formalités

Dans la dernière phrase de cet article remplacer les mots « ou qu'elle fait l'objet d'un examen en séance plénière » par les mots « et qu'elle fait l'objet d'un examen en séance plénière »

Exposé des motifs

Compte tenu du nombre de dossiers de formalités présentés par le secteur public (plus de 5000 par an) et du pourcentage important de dossiers relevant désormais du régime de la déclaration, notamment simplifiée, il est proposé de ne prévoir la transmission systématique au commissaire du gouvernement que des copies de dossiers de formalités du secteur public faisant l'objet d'un examen en séance plénière.

Chapitre II : Les déclarations Article 10 Délivrance des récépissés de déclarations

Compléter cet article par l'alinéa suivant

« Lorsqu'il existe un doute sur la conformité du traitement au régime de la déclaration, la Commission ou, par délégation le président ou le vice-président délégué, peut surseoir à la délivrance du récépissé. Le responsable du traitement est invité à fournir, dans un délai d'un mois, tous éléments de nature à justifier de la conformité du traitement au régime de la déclaration. »

Exposé des motifs

Cet amendement vise à réintroduire la possibilité pour la CNIL de surseoir à la délivrance du récépissé en cas de doute sur la conformité du traitement, comme le prévoit actuellement l'article 25 actuel du décret de 1978 pour les déclarations simplifiées. Le délai d'un mois permettrait notamment de vérifier qu'une déclaration n'est pas en réalité une demande d'autorisation.

Article 12 Dispense de déclaration

Rédiger ainsi le début de cet article

« Les normes d'exonération prises en application du II…(le reste sans changement) »

Exposé des motifs

Il est proposé, dans un souci de clarté et de meilleure compréhension des procédures, que la rédaction de cet article soit modifiée de façon à faire référence explicitement à des normes d'exonération, termes employés par le législateur non pas certes à l'article 24 mais à l'article 226-16-1 A du code pénal qui dispose que « Lorsqu'il a été procédé ou fait procéder à un traitement de données à caractère personnel dans les conditions prévues par le I ou le II de l'article 24 de la loi n° 78-17 du 6 janvier 1978 précitée, le fait de ne pas respecter, y compris par négligence, les normes simplifiées ou d'exonération établies à cet effet par la Commission nationale de l'informatique et des libertés est puni de cinq ans d'emprisonnement et de 300 000 € d'amende ».

Titre III : Du correspondant à la protection des données Article 40 La désignation du correspondant

Dans le paragraphe I de cet article, après les mots « avis de réception » insérer les mots « ou par remise au secrétariat de la commission contre reçu ».

Exposé des motifs

Cet amendement vise à assurer un parallélisme avec les formes de la notification des déclarations tel qu'il est prévu à l'article 7 du projet de décret.

Rédiger ainsi le premier alinéa du paragraphe II de cet article :

« II La notification comprend au moins les mentions suivantes : »

Exposé des motifs

Amendement de clarification.

Si la CNIL ne peut exiger d'autres éléments que ceux figurant dans la liste du II, il ne faut pas interdire au responsable du traitement de lui fournir plus d'informations sur les traitements concernés ou sur le correspondant lui-même.

Article 44 La tenue de la liste des traitements bénéficiant de la dispense

Rédiger ainsi le début du II de cet article :
« Dans le mois suivant sa désignation, …(le reste sans changement) »

Exposé des motifs

Le décalage dans le temps entre la prise d'effet de la dispense et la tenue de la liste pose le problème des traitements mis en œuvre au cours des trois mois prévus par le projet de décret. Dans la mesure où c'est le responsable de traitement qui communique au correspondant les éléments nécessaires à la tenue de la liste et que le correspondant n'a pas d'investigations à effectuer pour recenser les traitements, ce délai pourrait être réduit à un mois.

Rédiger ainsi la dernière phrase du dernier alinéa du paragraphe II de cet article :

« Pour les traitements déjà mis en œuvre à la date de la constitution de la liste, elle comporte la date et l'objet des mises à jour ainsi opérées. »

Exposé des motifs

L'article 44 ne prévoit pas que la liste tenue par le correspondant fasse état de la date et de l'objet des modifications substantielles apportées aux traitements. Si cela est admissible pour les traitements mis en œuvre avant l'entrée en fonction du correspondant (la CNIL a déjà recensé les traitements régulièrement déclarés), il n'en est pas de même pour les traitements postérieurs à la prise d'effet de la dispense.

Article 51 Le correspondant presse

Après les mots « l'article 42, » rédiger ainsi la fin du deuxième alinéa de cet article : « les 4° et 7° du II et le III de l'article 44 ainsi que le cinquième alinéa de l'article 45 du décret »

Exposé des motifs

Le deuxième alinéa de l'article 51 prévoit que le troisième alinéa de l'article 43 fixant une règle d'incompatibilité avec la qualité de responsable du traitement et les deuxième et troisième alinéas de l'article 45 fixant les missions du correspondant ne sont pas applicables au correspondant presse.

La possibilité de cumuler les fonctions de correspondant et celles de responsable de traitement prévue par le projet de décret est justifiée, semble t-il, par le fait qu'elle permettrait aux journalistes exerçant à titre individuel de bénéficier de la dispense en cumulant les deux fonctions. Or on peut estimer que ces journalistes sont de toute façon exonérés de déclaration.

L'article 67 de la loi a pour objet d'écarter l'application de plusieurs dispositions de la loi, notamment l'obligation de déclaration pour les traitements mis en œuvre aux seules fins d'expression littéraire et artistique et ceux aux fins d'exercice, à titre professionnel, de l'activité de journaliste dans le respect des règles déontologiques de cette profession.

Ces dérogations s'appliquent sans aucune restriction aux traitements ayant pour finalité l'expression littéraire et artistique. En revanche, pour les traitements ayant pour finalité l'activité journalistique, le législateur a prévu une contrepartie : la nomination d'un correspondant « appartenant à un organisme de presse écrite ou audiovisuelle ». Cette contrepartie s'applique-t-elle à tous les traitements ayant pour finalité l'activité journalistique ?

On peut penser que le législateur n'a pas réellement entendu soumettre à ce mécanisme lourd les fichiers individuels, par exemple les carnets d'adresse des journalistes, mais seulement les traitements mis en œuvre collectivement par un organe de presse (bases de données documentaires, archivage des contenus publiés…). Quel est l'intérêt qu'un journaliste se désigne correspondant de lui-même et tienne une liste de ses fichiers, liste au surcroît inaccessible à toute personne ?

La Commission estime que le journaliste ou le photographe, soit pour l'ensemble de ses fichiers s'il exerce de manière indépendante soit pour les fichiers

dont il est le seul maître s'il exerce au sein d'une entreprise de presse, bénéficie sans conditions de la dispense et n'a pas à désigner de correspondant. Elle considère que seuls les organismes de presse sont donc concernés par la désignation du correspondant.

Il n'y a en conséquence pas lieu de prévoir d'aménagement spécifique destiné à écarter la règle d'incompatibilité avec le responsable du traitement et ce d'autant que les dispositions relatives à l'absence de conflit d'intérêt sont applicables au correspondant.

Corrélativement doivent être également supprimées les exclusions qui résultent de la possibilité de cumul : les deuxième et troisième alinéas de l'article 45.

Cet amendement vise donc à réintroduire une règle d'incompatibilité entre la qualité de correspondant presse et celle de responsable du traitement et d'en tirer toutes les conséquences.

Contrairement à ce que prévoit le projet de décret, seraient donc applicables au correspondant presse les dispositions suivantes :

- 1er alinéa de l'article 43 : Le correspondant à la protection des données exerce sa mission directement auprès du responsable des traitements.
- 3ème alinéa de l'article 43 : Le responsable des traitements ou son représentant légal ne peut être désigné comme correspondant.
- 2ème alinéa de l'article 45 : A cette fin, il peut faire toute recommandation au responsable des traitements.
- 3ème alinéa de l'article 45 : Il est consulté, préalablement à leur mise en oeuvre, sur l'ensemble des nouveaux traitements appelés à figurer sur la liste prévue par le I de l'article 44 du présent décret.

Titre IV : Des pouvoirs de la Commission Chapitre Ier : Contrôles et vérifications Article 54 Procès-verbal

Rédiger ainsi le troisième alinéa de cet article :

« Lorsque la visite ne peut se dérouler en raison de l'absence du responsable des lieux ou de la personne qu'il a désignée pour le remplacer ou en raison de l'opposition du responsable des lieux, mention en est faite dans le procès-verbal. »

Exposé des motifs

L'absence du responsable des lieux ne peut faire obstacle à une visite si le responsable a désigné une personne qui exerce, en son absence, la responsabilité de l'accès aux lieux. Il est donc proposé de préciser que seule l'absence du responsable ou de son préposé conduit à un procès-verbal de carence.

Article 57 Experts

Rédiger ainsi le début du II de cet article :

« II. – Lorsque les opérations de vérifications nécessitent la communication de données médicales ...(le reste sans changement) »

En conséquence, à la fin de la première phrase, remplacer les mots « la communication de ces données » les mots « cette communication »

Exposé des motifs

La CNIL estime être en droit de conduire des contrôles sur des traitements contenant des données médicales individuelles sans la présence d'un médecin dès lors qu'elle ne sollicite pas la communication des documents consultés. Or le décret a pris un parti contraire en retenant le critère le plus large d'accès à des données médicales. Il est proposé de s'en tenir à la lettre de l'article 44 et donc au terme de communication.

Après la première phrase du II de cet article, insérer la phrase suivante :

« Le président de la commission peut également demander le concours d'un médecin figurant sur une liste établie par le Conseil national de l'Ordre des médecins. »

Exposé des motifs

La procédure de désignation prévue par le projet de décret nécessite que le président de la Commission demande au préfet territorialement compétent de désigner un médecin inspecteur de santé publique ou un médecin inspecteur du travail. Cette solution présente deux inconvénients principaux :

- elle subordonne l'action de la CNIL à la bonne volonté du Préfet, aux délais nécessaires pour procéder à la désignation d'un médecin, et à la disponibilité de ce dernier ;
- elle empêche la sensibilisation - voire la spécialisation - du professionnel désigné aux problématiques « Informatique et libertés » ;

Il serait préférable de mettre en place concurremment une procédure permettant à la CNIL de désigner un médecin, comme cela est prévu de manière générale par le paragraphe I pour les experts. Toutefois elle ne pourrait choisir qu'un médecin figurant sur une liste établie par le Conseil national de l'Ordre des médecins.

Section 5 : Secret professionnel Article 58 Secret professionnel

Dans cet article remplacer les mots « , le cas échéant, de tout élément porté à la connaissance des personnes chargées du contrôle » par les mots « des dispositions législatives ou règlementaires auxquelles elle se réfère ainsi que des catégories de données ou de fichiers qu'elle estime couverts par ces dispositions. »

Exposé des motifs

Il s'agit de préciser le texte de cet article pour que l'opposition du secret professionnel se fasse dans des conditions claires permettant à la CNIL d'agir, le cas échéant, sur le terrain du délit d'entrave.

Chapitre II : Sanctions administratives Article 59 Le fonctionnement général de la formation restreinte

Dans la première phrase du I de cet article, remplacer les mots « à la majorité de neuf voix » par les mots « à la majorité absolue des membres composant la commission »

Exposé des motifs

Le I de cet article dispose que les membres élus de la formation restreinte le sont à la majorité de neuf voix. Ces membres siègeront donc avec le président et les vice-présidents qui eux sont élus à la majorité absolue des membres composant la Commission. Cette asymétrie dans laquelle l'élection du président semble avoir moins d'importance que celle des membres de la formation restreinte n'est pas acceptable. Il est proposé d'harmoniser l'article 59 avec l'article 2.

1 Dans la première phrase du premier alinéa du I de cet article, supprimer le mot « titulaires »

2 Supprimer la deuxième phrase du premier alinéa du I de cet article

Exposé des motifs

Le I de l'article 59 du projet de décret prévoit aussi l'élection supplémentaire de trois suppléants aux trois membres titulaires élus. Or, l'élection de suppléants n'est pas prévue par la loi du 6 août 2004.

Cette disposition est non seulement inutile dans la mesure où le II de l'article 59 du projet de décret prévoit une règle de quorum aux termes de laquelle la formation restreinte ne peut valablement délibérer que si au moins quatre de ses membres, dont le Président ou le vice-président délégué, sont présents mais dangereuse. L'élection de trois suppléants implique que, sur les dix-sept commissaires composant la Commission, neuf appartiendraient à la formation restreinte (le président, les deux vice-présidents, les trois titulaires et leurs trois suppléants). Ainsi, seuls huit commissaires pourraient être désignés pour rapporter devant la formation restreinte lorsqu'une procédure est engagée tandis que neuf autres seraient incités à ne pas prendre par aux contrôles et peut-être à ne pas suivre de secteurs. Le risque est de créer une césure entre deux moitiés de la Commission, l'une composée de « juges du siège » et l'autre étant le « parquet » de la Commission.

Dans le deuxième alinéa du I de cet article, remplacer les mots « si douze membres sont présents » par les mots « si la majorité des membres en exercice de la commission participe à la séance.»

Exposé des motifs

Alignement du quorum exigé pour l'élection des trois membres de la formation restreinte sur la règle fixée par l'article 2 pour l'élection des autres membres de la formation restreinte, le président et les vice-présidents

Article 64 La procédure préalable au prononcé d'une sanction

Rédiger ainsi le début du deuxième alinéa de cet article : « Le rapporteur procède à toutes diligences utiles avec le concours des services de la commission. Le responsable du traitement …(le reste sans changement) »

Exposé des motifs

Amendement rédactionnel. Le caractère optionnel du concours prêté par les services de la CNIL au rapporteur ne correspond pas à la réalité du fonctionnement de la CNIL

Dans la troisième phrase du deuxième alinéa de cet article, supprimer les mots « à sa demande ou »

Exposé des motifs

Au cours de la phase d'instruction, le responsable du traitement peut demander à être entendu. S'agissant d'une audition préalable à toute procédure contradictoire, on peut s'interroger sur le point de savoir comment le responsable du traitement pourrait demander à être entendu, avant même la rédaction du rapport. En effet, il n'est a priori, à ce stade, pas encore informé qu'une procédure de sanction est susceptible d'être engagée.

Il est donc proposé de supprimer les mots « à sa demande ou », c'est à dire de laisser l'initiative d'une éventuelle audition au rapporteur.

Rédiger ainsi le III de cet article :

«III Le responsable du traitement est informé de la date de la séance de la commission à l'ordre du jour de laquelle est inscrite l'affaire le concernant et de la faculté qui lui est offerte d'y être entendu, lui-même ou son représentant, par lettre recommandée avec demande d'avis de réception, ou remise en main propre contre récépissé ou acte d'huissier. Cette lettre doit lui parvenir au moins un mois avant ladite date.»

Exposé des motifs

Le III prévoit que le responsable du traitement est convoqué à la séance à laquelle son affaire est examinée. Or la CNIL dans son règlement intérieur (décembre 2004) a considéré que le responsable du traitement avait la faculté d'être entendu s'il le souhaitait. Il est proposé d'adopter une rédaction soulignant ce caractère facultatif qui n'apparaît pas clairement dans le projet de décret.

dir="ltr">Article 65 Déroulement de la séance lors du prononcé d'une sanction

Dans le deuxième alinéa du paragraphe III de cet article, remplacer les mots « à compter du jour où la sanction est devenue définitive » par les mots « à compter du jour où la sanction a été prononcée. »

Exposé des motifs

L'article 65 du projet de décret prévoit, dans son III, que la publication de la sanction décidée par la Commission ne peut intervenir que si la décision de sanction est devenue définitive. Ainsi, en cas de recours, il est important de souligner que la CNIL ne pourra pas publier la sanction prononcée. Cette restriction de publication ne paraît pas conforme à l'esprit de la loi et à la volonté du législateur, tels qu'ils ressortent des débats devant l'Assemblée nationale à l'occasion de l'adoption de la loi. Il est donc proposé de supprimer cette disposition.

Titre V : Dispositions pénales Article 70 Insertion dans le code pénal des contraventions à la loi du 6 janvier 1978

Rédiger ainsi le début de l'article R 625-10 du code pénal :

Article R.625-10

« Art. R. 625-10. - Hors les cas où cette information n'est pas exigée par la loi, est puni de l'amende prévue pour les contraventions de la cinquième classe le fait, pour le responsable d'un traitement automatisé à caractère personnel ou son représentant :

« 1° De ne pas informer la personne auprès de laquelle sont recueillies des données à caractère personnel la concernant :

«- De l'identité du responsable du traitement et, le cas échéant, de celle de son représentant ;

« - De la finalité poursuivie par le traitement auquel les données sont destinées ;

« - Du caractère obligatoire ou facultatif des réponses ;

« - Des conséquences éventuelles, à son égard, d'un défaut de réponse ;

« - Des destinataires ou catégories de destinataires des données ;

« - De ses droits d'opposition, d'interrogation, d'accès et de rectification.

«- Le cas échéant, des transferts de données à caractère personnel envisagés à destination d'un Etat non membre de la Communauté européenne.

« 2° Lorsque les données sont recueillies par voie de questionnaire, de ne pas porter sur le questionnaire les informations relatives :

«- à l'identité du responsable du traitement et, le cas échéant, de celle de son représentant ;

« - à la finalité poursuivie par le traitement auquel les données sont destinées ;

« - au caractère obligatoire ou facultatif des réponses ;

« - aux droits d'opposition, d'interrogation, d'accès et de rectification des personnes auprès desquelles sont recueillies les données.

3° …(le reste sans changement) »

Exposé des motifs

La rédaction de l'article 32 de la loi conduit à distinguer deux infractions différentes :

- le fait de ne pas informer des points 1° à 7° du I de l'article 32 de la loi quand la collecte se fait oralement ou par voie de questionnaire ;
- le fait que les mentions d'information correspondant aux points 1° (identité du responsable du traitement), 2° (finalité), 3° (caractère obligatoire ou facultatif des réponses) et 6° (droits d'opposition, d'accès,

de rectification) du même article, quand la collecte se fait par voie de questionnaire, ne figurent pas sur le questionnaire.

Titre VI : Dispositions particulières aux traitements relevant des articles 26 et 42 de la loi susvisée du 6 janvier 1978 Article 72 Habilitation des agents de la CNIL

Supprimer le paragraphe II de cet article

Exposé des motifs

Le paragraphe II prévoit que les agents de la commission et les personnes lui prêtant leur concours, appelés à effectuer les visites ou les vérifications portant sur les traitements intéressant la sûreté de l'Etat, la défense ou la sécurité publique ou qui ont pour objet la prévention, la recherche ou la constatation des infractions pénales, devraient y être habilités par le président de la commission sur la base d'une enquête administrative favorable menée par le Premier ministre, dans les conditions prévues par la loi susvisée du 21 janvier 1995.

S'il s'agit de soumettre les agents de la CNIL appelés à accéder dans le cadre de leurs missions de vérifications à des conditions d'habilitation analogues à celles prévues pour les personnels de police et de gendarmerie appelés à accéder aux fichiers de police judiciaire et qui doivent, aux termes de l'article 21 IV de la loi du 18 mars 2003, être « spécialement habilités », une telle assimilation paraît tout à fait inappropriée, l'accès ponctuel des agents de la CNIL ne s'effectuant absolument pas pour les mêmes raisons et dans les mêmes conditions que l'accès permanent des services de police et de gendarmerie. En outre, lorsqu'il s'agit de vérifications faites dans le cadre du droit d'accès indirect, elles sont toujours menées sous la direction d'un membre de la CNIL ayant la qualité de magistrat.

Appliquer une telle procédure d'habilitation aux agents de la CNIL au titre des « zones protégées » paraît tout aussi inapproprié, l'accès à ces zones protégées n'étant susceptible de s'effectuer que de façon ponctuelle et en tout état de cause contrôlée puisque les visites et vérifications de la CNIL s'effectuent toujours en présence de représentants des responsables de traitements. En outre, les fichiers les plus sensibles (DGSE notamment) ne peuvent de toute manière faire l'objet d'un contrôle sur place par la CNIL puisque l'article 44, IV de la loi de 1978 modifiée, les exclut de cette procédure.

Dans la mesure où l'article 52 du projet de décret prévoit déjà que les agents de la CNIL appelés à faire des contrôles ne doivent pas avoir fait l'objet d'une condamnation à une peine correctionnelle ou criminelle inscrite au bulletin n°2 du casier judiciaire, il est proposé de supprimer le paragraphe II.

Article 74 Exercice du droit d'accès

Rédiger ainsi la première phrase du deuxième alinéa du II de cet article :

« Le responsable du traitement dispose pour réaliser ses investigations d'un délai de trois mois à partir de la date de réception de la transmission par la commission de la demande d'accès. »

Exposé des motifs

Le délai de trois mois dont disposerait le responsable du traitement pour lui permettre de réaliser ses investigations (c'est-à-dire recherche des fiches et des dossiers tant au niveau des services locaux qu'au plan local, organisation des séances d'investigation, réponses aux demandes éventuelles de rectification et de suppression…) partirait qu'à compter de la date à laquelle la CNIL aurait informé le responsable du traitement de la désignation de l'un de ses membres pour mener les investigations utiles.
Or, en pratique la désignation du commissaire n'intervient qu'à la fin du processus d'instruction des demandes par le responsable du traitement, concrètement, lorsque les services de la CNIL sont informés par le responsable du traitement qu'il existe bien une fiche ou un dossier au nom du requérant et que ce dossier peut être vérifié dans ses locaux.

Dès lors, pour que ce délai ait un sens, il apparaît impératif de proposer que ce délai parte à compter de la transmission par la CNIL au responsable du traitement de la demande de droit d'accès indirect.

Après les mots « a prévu » rédiger ainsi la fin du premier alinéa du paragraphe VII de cet article : « les conditions dans lesquelles il serait fait application de l'article 41 de la même loi. »

Exposé des motifs

Le paragraphe VII. prévoit, conformément à l'article 42 de la loi, que les dispositions du présent article sont applicables aux traitements mis en œuvre par les administrations publiques et les personnes privées chargées d'une mission de service public qui ont pour mission de prévenir, rechercher ou constater des infractions, ou de contrôler ou recouvrer des impositions, si l'autorisation mentionnée aux articles 25, 26 ou 27 de la loi susvisée du 6 janvier 1978 a prévu que le droit d'accès s'exercerait dans les conditions de l'article 41 de la même loi.

Cette formulation donne à penser que le texte de l'autorisation ne pourra que prévoir l'application générale de l'article 41, sans autre précision. Or, il serait préférable que l'autorisation puisse être éventuellement

plus précise sur les conditions dans lesquelles la procédure du droit d'accès indirect trouvera à s'appliquer. En outre, cette solution présenterait l'avantage de tenir compte du 4e alinéa de l'article 41 qui dispose que l'autorisation des articles 25, 26 ou 27 peut prévoir que certaines informations sont directement communiquées au requérant.

Titre VII : Dispositions finales Article 76 Abrogation de divers textes réglementaires

Rédiger ainsi le II de cet article :

« Dans le deuxième alinéa de l'article 7 du décret susvisé du 14 octobre 1991, les mots « l'article 39 » sont remplacés par les mots « l'article 41 ».

Exposé des motifs

Le II de l'article 76 abroge l'article 7 du décret n° 91-1051 du 14 octobre 1991 sur les fichiers des services des renseignements généraux qui fixe les modalités du droit d'accès indirect propres à ce fichier et le remplace par une référence aux modalités générales du droit d'accès indirect telles qu'elles sont fixées à l'article 74 du présent décret.

Cette abrogation a notamment pour effet de supprimer la référence faite dans le décret de 1991 à deux catégories de personnes [personnes ayant une autorisation d'accès à des informations protégées ; personnes jouant un rôle politique, économique, social ou religieux significatif], pour lesquelles le principe de la communication des informations est affirmé.
Mais au delà de cette différence de rédaction, c'est une question plus fondamentale qui est posée : les modalités du droit d'accès indirect sont-elles fixées par un texte général (article 74 du décret) une fois pour toutes, c'est à dire pour l'ensemble des fichiers relevant de l'article 41 de la loi, ou, cas par cas, par des dispositions spécifiques figurant dans l'acte règlementaire créant le fichier qui est soumis pour avis à la CNIL ?

Si cette deuxième hypothèse est désormais écartée, comme semblent le montrer la rédaction du II du présent article mais aussi celle des III, IV, V et VI (cf. amendements ci-dessous), cela signifie que la CNIL, saisie pour avis d'un projet de fichier de police, ne se prononce plus sur les conditions du droit d'accès, c'est à dire sur l'aménagement des règles générales prévues par la loi et son décret d'application. Or l'examen de ces conditions est un élément substantiel de l'avis de la CNIL de même que ces conditions sont un élément consubstantiel de la définition de tels fichiers. La CNIL ne peut accepter que le champ de son intervention au titre de l'article 26 de la loi du 6 janvier 1978 soit ainsi réduit.

Rédiger ainsi le premier alinéa du III de cet article :

« Dans l'article 6 du décret susvisé du 6 mai 1995, les mots « l'article 39 » sont remplacés par les mots « l'article 41 ».

Exposé des motifs

Le premier alinéa du III abroge l'article 6 du décret no 95-577 du 6 mai 1995 relatif au système informatique national du système d'information Schengen (N-SIS). Cet article 6 prévoit actuellement :
« Le droit d'accès aux informations visées à l'article 4 s'exerce auprès de la Commission nationale de l'informatique et des libertés, conformément aux articles 109 et 114 de la convention et à l'article 39 de la loi du 6 janvier 1978 susvisée sans préjudice des dispositions réglementaires relatives aux données susceptibles d'être consultées directement par l'intéressé exerçant ce droit. »
Il renvoie donc aux actes réglementaires qui régissent le fichier des personnes recherchées (FPR) et le fichier des véhicules volés (FVV) d'où proviennent les données françaises du N-SIS et donc à des règles particulières de droit d'accès qui ne peuvent être ainsi balayées et remplacées par une référence aux règles générales de l'article 74 du décret.

La réécriture de l'article 6 devrait donc au minimum reprendre les limitations au droit d'accès indirect apportées par les textes en vigueur. Il est donc proposé de se limiter à remplacer dans l'article 6 du décret la référence à l'article 39 de la loi de 1978 ancienne version par une référence à l'article 41 nouvelle version.

Supprimer le V de cet article

Exposé des motifs

Le V concerne le décret n°2001-583 du 5 juillet 2001 relatif au STIC dont l'article 8 dispose :

« Le droit d'accès s'exerce d'une manière indirecte, dans les conditions prévues à l'article 39 de la loi du 6 janvier 1978 susvisée, par demande portée préalablement devant la Commission nationale de l'informatique et des libertés, pour l'ensemble des données.
Toutefois, la commission peut constater, en accord avec le ministère de l'intérieur, que des informations nominatives enregistrées ne mettent pas en cause la sûreté de l'État, la défense ou la sécurité publique et qu'il y a donc lieu de les communiquer à la personne intéressée, sous réserve que la procédure soit judiciairement close et après accord du procureur de la République. »

Le V est une parfaite illustration de la question de principe évoquée à propos du II.

Le STIC fait actuellement l'objet d'un projet de modification de ce même décret soumis à la CNIL qui a demandé notamment une refonte de cet article 8 faisant application du dernier alinéa de l'article 41 de la loi du 6 janvier modifiée en ce qui concerne les données relatives aux victimes. La CNIL ne peut donc admettre que ce texte soit modifié parallèlement au dossier dont elle est saisie et en dehors du cadre de l'examen particulier auquel elle entend se livrer. Il est donc proposé de supprimer le paragraphe V.

Rédiger ainsi le premier alinéa du VI de cet article :

« A l'article 5 de l'arrêté du 23 avril 1993 relatif au Fichier national informatisé de documentation de la direction générale des douanes et droits indirects, les mots « l'article 34 » sont remplacés par les mots : « l'article 39 » et les mots « l'article 39 » sont remplacés par les mots : «l'article 41 ».

Exposé des motifs

Le VI concerne l'arrêté du 23 avril 1993 relative au FNID de la direction des douanes, dont l'article 5 qui serait réécrit prévoit actuellement que le droit d'accès est régi par principe par l'article 34 de la loi du 6 janvier mais que la DGDDI peut transmettre à la Commission la requête qui lui a été présentée, lorsqu'elle estime que les informations demandées intéressent la sûreté de l'État, la défense ou la sécurité publique et relèvent de ce fait de la procédure du droit d'accès indirect de l'article 39 ou sont couverte par un secret relevant d'une convention internationale. Il appartient alors à la CNIL de délimiter les données qui peuvent être communiquées et celles qui relèvent de l'article 39.

Le même dispositif a été si peu contesté par la douane à ce jour qu'il a été repris tout récemment dans l'arrêté du 1er juillet 2003 créant le nouveau traitement national de la douane qui se substituera au FNID, le SILCF (non visé à l'article 76…).

Il est donc proposé de s'en tenir à des modifications de pure coordination.

Le président, Alex Türk

Décret n° 2005-1309 du 20 octobre 2005 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n° 2004-801 du 6 août 2004 J.O n° 247 du 22 octobre 2005 page 16769, texte n° 31 - NOR: JUSC0520586D

Référence : C.N.I.L, délibération du 24 mars 2005, *N°2005-049 RELATIVE À L'ADOPTION DU DÉCRET D'APPLICATION DE LA LOI N° 2004-801*, DROIT-TIC http://www.droit-tic.com/juris/aff.php?id_juris=59

DROIT-TIC .com

R.D.T.I.C

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

DÉLIBÉRATION

N° 2005-296

22 novembre 2005

Adoption d'une norme simplifiée relative aux traitements automatisés de données à caractère personnel mis en œuvre par les membres des professions médicales et paramédicales exerçant à titre libéral à des fins de gestion de leur cabinet

Thèmes

Informatique et libertés, Loi applicable et juridiction compétente

Abstract

Informatique et libertés, traitements automatisés de données à caractère personnel, professions médicales et paramédicales, finalté de gestion, Formalités simplifiées

Résumé

Norme simplifiée relative aux traitements automatisés de données à caractère personnel mis en œuvre par les membres des professions médicales et paramédicales exerçant à titre libéral à des fins de gestion de leur cabinet

Délibération n°2005-296 du 22 novembre 2005 portant adoption d'une norme simplifiée relative aux traitements automatisés de données à caractère personnel mis en œuvre par les membres des professions médicales et paramédicales exerçant à titre libéral à des fins de gestion de leur cabinet

La Commission nationale de l'informatique et des libertés,

Vu la convention n°108 du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

Vu 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 notamment son article 8;

Vu la loi n°78-17 du 6 janvier 1978 modifiée par la loi n° 2004-810 du 6 août 2004 relative à l'informatique, aux fichiers et aux libertés notamment ses articles 11, 22, 23, 24 I et 30 ;

Vu les articles 226-13 et 226-14 du code pénal relatifs au secret professionnel ;

Vu le code de la santé publique et notamment son article L. 1111-8 ;

Vu les articles L. 161-29, R. 115-1 et suivants et R. 161-47 du code de la sécurité sociale ;

Vu le décret n°2005-1309 du 20 octobre 2005 pris pour l'application de la loi du 6 janvier 1978 modifiée par la loi n°2004-810 du 6 août 2004 ;

Vu le décret n° 95-100 du 6 septembre 1995 portant code de déontologie médicale ;

Vu le décret 93-221 du 16 février 1993 relatif aux règles professionnelles des infirmiers et infirmières ;

Vu le décret 91-776 du 8 août 1991 portant code de déontologie des sages femmes ;

Vu le décret n° 67-671 du 22 juillet 1967 modifié portant code de déontologie des chirurgiens-dentistes;

Vu la délibération n° 97-008 du 4 février 1997 portant adoption d'une recommandation sur le traitement des données à caractère personnel ;

En vertu de l'article 24 de la loi du 6 janvier 1978 modifiée, la Commission nationale de l'informatique et

des libertés est habilitée à établir des normes destinées à simplifier l'obligation de déclaration des traitements les plus courants et dont la mise en œuvre, dans des conditions régulières, n'est pas susceptible de porter atteinte à la vie privée ou aux libertés.

Les traitements informatisés de données à caractère personnel mis en œuvre par les membres des professions médicales et paramédicales exerçant à titre libéral à des fins de gestion de leur cabinet sont de ceux qui peuvent, sous certaines conditions, relever de cette définition.

Décide : Article 1er
Champ d'application

Peuvent bénéficier de la procédure de la déclaration simplifiée de conformité à la présente norme les traitements mis en œuvre par les membres des professions médicales et paramédicales exerçant à titre libéral qui répondent aux conditions définies aux articles 1 à 9 ci-après.

La présente norme ne s'applique ni aux traitements mis en œuvre par les pharmacies, ni aux traitements des laboratoires d'analyses de biologie médicale.

En cas de dépôt chez un hébergeur des données de santé, le traitement mis en oeuvre par le professionnel de santé ne peut être déclaré par référence à la présente norme.

Article 2
Finalités du traitement

Les traitements sont mis en œuvre pour faciliter la gestion administrative des cabinets et l'exercice des activités de prévention, de diagnostics et de soins.

Ils n'assurent pas d'autres fonctions que :

- la gestion des rendez-vous ;
- la gestion des dossiers médicaux et l'édition des ordonnances ;
- la gestion et la tenue des dossiers individuels de soins ;
- l'établissement et la télétransmission des feuilles de soins ;
- l'envoi de courriers aux confrères ;
- la tenue de la comptabilité ;
- la réalisation d'études statistiques à usage interne ;

Les données personnelles de santé ne peuvent être utilisées que dans l'intérêt direct du patient et, dans les conditions déterminées par la loi, pour les besoins de la santé publique. Toute autre exploitation de ces données, notamment à des fins commerciales est proscrite.

La constitution et l'utilisation à des fins de prospection ou de promotion commerciales de fichiers composés à partir de données issues directement ou indirectement des prescriptions médicales ou des informations médicales sont interdites, dès lors que ces fichiers permettent d'identifier directement ou indirectement un professionnel de santé.

Article 3
Informations collectées et traitées Les informations suivantes peuvent être collectées :
a) identité : nom, prénom, date de naissance, adresse, numéro de téléphone ; b) numéro de sécurité sociale : pour l'édition des feuilles de soins et la télétransmission aux caisses d'assurance maladie dans les conditions définies par les articles R. 115-1 et suivants du code de la sécurité sociale ;
c) situation familiale : situation matrimoniale, nombre d'enfants, nombre de grossesses ;
d) vie professionnelle : profession, conditions de travail ; e) santé : historique médical, historique des soins, diagnostics médicaux, traitements prescrits, nature des actes effectués et tout élément de nature à caractériser la santé du patient et considéré comme pertinent par le professionnel de santé. Des informations relatives aux habitudes de vie peuvent être collectées avec l'accord du patient et dans la stricte mesure où elles sont nécessaires au diagnostic et aux soins.

Article 4
Destinataires des informations

- Afin d'assurer la continuité des soins et avec l'accord de la personne concernée, les professionnels de santé et dans les établissements de santé, les membres de l'équipe de soins, chargés de la prise en charge du patient peuvent être destinataires des données figurant dans l'application.
- Les personnes affectées à la gestion du secrétariat n'ont accès, dans le respect des dispositions sur le secret professionnel, qu'aux informations relatives à la gestion du cabinet et en particulier à la gestion des rendez-vous.
- Afin de permettre le remboursement des actes, des prestations et leur contrôle, les personnels des organismes d'assurance maladie ont connaissance, dans le cadre de leurs fonctions et pour la durée nécessaire à l'accomplissement de celles-ci, de l'identité de l'assuré, de son numéro de sécurité sociale et du code des actes effectués et des prestations servies. Outre ces données, les médecins

conseils des caisses accèdent au code des pathologies diagnostiquées dans les conditions définies à l'article L. 161-29 du code de la sécurité sociale.

- Les personnels des organismes d'assurance maladie complémentaire sont destinataires dans le cadre de leurs attributions, de l'identité de leurs assurés, de leur numéro de sécurité sociale et sous la forme de codes regroupés, aux catégories des actes et prestations effectués.
- Les organismes de recherche dans le domaine de la santé et les organismes spécialisés dans l'évaluation des pratiques de soins peuvent être destinataires de données personnelles de santé dans les conditions définies par la loi du 6 janvier 1978 modifiée.

Article 5
Durée de conservation

Les informations enregistrées ne peuvent être conservées dans l'application au-delà d'une durée de cinq ans à compter de la dernière intervention sur le dossier du patient. A l'issue de cette période, elles sont archivées sur un support distinct et peuvent être conservées pendant quinze ans dans des conditions de sécurité équivalentes à celles des autres données enregistrées dans l'application.

Les doubles des feuilles de soins électroniques doivent être conservées 90 jours conformément à l'article R 161-47 du code de la sécurité sociale.

Article 6
Information et droit d'accès

Conformément aux dispositions à la loi du 6 janvier 1978 modifiée par la loi du 6 août 2004, les personnes dont les données sont enregistrées et conservées dans le fichier du cabinet sont informées, par un document affiché dans les locaux du cabinet médical ou para-médical ou remis en main propre, de l'identité du responsable du traitement, de sa finalité, des destinataires des informations et des modalités pratiques d'exercice de leurs droits, en particulier du droit d'accès aux informations qui les concernent.

Article 7
Politique de confidentialité et sécurités

Des mesures de sécurité physique et logique sont mises en place afin de préserver la confidentialité des informations couvertes par le secret médical et empêcher qu'elles ne soient déformées, endommagées ou communiquées à des tiers non autorisés.

Le professionnel de santé accède à l'application en utilisant sa carte de professionnel de santé. Les personnels placés sous l'autorité du professionnel de santé doivent également disposer d'une carte d'accès personnelle ou d'un mot de passe personnel.

En cas d'utilisation du réseau internet pour transmettre des données personnelles de santé, un système de chiffrement « fort » de la messagerie doit être mis en place. En outre, un antivirus doit être installé et mis à jour régulièrement afin de se prémunir des risques de captation des données.

Le professionnel de santé précise par écrit, dans un protocole de confidentialité, les mesures effectivement mises en œuvre. Ce protocole est communiqué à la CNIL à sa demande.

Article 8

La présente délibération sera publiée au journal officiel de la République française.

Le Président Alex Türk

Voir aussi :

CNIL, Echos des séances, Simplification de la déclaration des logiciels de gestion des cabinets médicaux et paramédicaux, 21 déc. 2005

Référence : C.N.I.L, délibération du 22 novembre 2005, *N°2005-296 PORTANT ADOPTION D'UNE NORME SIMPLIFIÉE RELATIVE AUX TRAITEMENTS AUTOMATISÉS DE DONNÉES À CARACTÈRE PERSONNEL MIS EN ŒUVRE PAR LES MEMBRES DES PROFESSIONS MÉDICALES ET PARAMÉDICALES*, DROIT-TIC
http://www.droit-tic.com/juris/aff.php?id_juris=60