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

ANALYSES

DELIBERATIONS CNIL

TEXTE OFFICIEL

© Julien Le Clainche

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

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

Informations légales

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

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

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

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

Vous pouvez présenter vos observations, remarques, 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

© Julien Le Clainche

DROIT-TIC .com

R.D.T.I.C

LA REVUE DU DROIT DES TECHNIQUES DE L'INFORMATION ET DE LA COMMUNICATION-
N°57 – OCTOBRE 2006

ANALYSES

DÉLIBÉRATIONS CNIL

TEXTE OFFICIEL

DROIT-TIC.com

R.D.T.I.C

LA REVUE DU DROIT DES TECHNIQUES DE L'INFORMATION ET DE LA COMMUNICATION-
N°57 – OCTOBRE 2006

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

QUAND REPRODUCTION A L'IDENTIQUE NE RIME PAS AVEC CONTREFACON

Par M. Benjamin Vitasse, juriste noms de domaine, MailClub.info

Le 10 octobre 2006, la Cour d'Appel de Rennes a rendu une décision des plus intéressantes qui précise encore un peu plus la frontière entre le droit des marques et la sphère des noms de domaine.

Cette décision oppose la société Icodia (hébergeur de sites web) à la société Acréat (créateur de sites internet).

Icodia s'est vue poursuivie en justice pour avoir enregistré le nom de domaine « acreat.fr ». La société Acréat estimait que ce nom de domaine constituait une contrefaçon de sa marque « acreat ».

Reproduire n'est pas contrefaire

Le titulaire d'une marque sera tenté d'agir à l'encontre d'un nom de domaine reproduisant celle-ci. Pour autant, la réservation d'un nom de domaine similaire à une marque ne sera contrefaisante que si les produits ou services proposés par le site sont similaires ou identiques à ceux correspondant aux classes de produits visés lors de l'enregistrement de la marque.

La société Acréat avait enregistrée sa marque dans la classe 38 (qui vise les services de télécommunication), se croyant ainsi prémunie contre un dépôt de nom de domaine qui viendrait à reproduire sa marque.

Si un site internet est effectivement un service de télécommunication, les juges rappellent que la contrefaçon s'évalue au regard des produits et services proposés par le site. En l'espèce, la contrefaçon n'a pu être reconnue, notamment car l'activité de création de sites (société Acréat) n'était pas similaire à celle de la société Icodia (hébergement de sites internet).

Dépôt sans réelle utilisation

Les juges ont par ailleurs relevé l'absence d'utilisation réelle du nom de domaine litigieux par la société Icodia. Cette décision rappelle au passage un arrêt de la cour de cassation du 13 décembre 2005 statuant que *« la réservation d'un nom de domaine en soi, sans utilisation réelle de ce nom de domaine ne constitue pas un acte de contrefaçon »*.

Absence de risque de confusion

Enfin, les juges ont relevé *« qu'un nom de domaine ne peut contrefaire par reproduction ou par imitation une marque antérieure, peu important que celle-ci soit déposée en classe 38, pour désigner des services de communication télématique, que si les produits et services offerts sur ce site sont soit identiques, soit similaires à ceux visés pour l'enregistrement de la marque et de nature à entraîner un risque de confusion dans l'esprit du public »*.

En l'espèce, la société Acréat ne rapporte pas la preuve d'un usage contrefaisant de nature à entraîner un risque de confusion. Icodia avait même contacté la société Acréat en se proposant de retirer le nom de domaine. L'absence de réponse de la part d'Acréat a naturellement été interprétée par la Cour comme une autorisation implicite de sa part.

En définitive la société Icodia a pu conserver l'usage de « acreat.fr ».

L'intérêt de cette décision réside dans la stricte application du principe de spécialité qui fait donc apparaître la possible coexistence entre une marque antérieure et un nom de domaine identique à celle-ci.

Pour en savoir plus :

Arrêt Soficar/Le tourisme moderne compagnie parisienne de tourisme, n° de pourvoi 04-10.143 Dalloz 2006 n°1 p.63-64 pièce n°18)

http://www.legalis.net/article.php3?id_article=1555

DROIT-TIC .com

R.D.T.I.C

LA REVUE DU DROIT DES TECHNIQUES DE L'INFORMATION ET DE LA COMMUNICATION-
N°57 – OCTOBRE 2006

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

L'OMPI TRANCHE SON 25000IÈME NOM DE DOMAINE LITIGIEUX

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

Le Centre d'arbitrage et de médiation de l'Organisation Mondiale de la Propriété Intellectuelle (OMPI) a atteint le chiffre de 25 000 litiges réglés en sept ans d'existence. Des décisions en faveur des plaignants

Le Centre d'arbitrage et de médiation de l'Organisation Mondiale de la Propriété Intellectuelle (OMPI) a atteint le chiffre de 25 000 litiges réglés en sept ans d'existence. Des décisions en faveur des plaignants

L'OMPI traite les plaintes selon les Principes directeurs concernant le règlement uniforme des litiges relatifs aux noms de domaine (principes UDRP) et diverses autres procédures. La 25 000e affaire concerne le cybersquatting de redlionhotels.com, transmis au propriétaire de la marque, la chaîne Red Lion Hotels.

Un cas classique, sachant que sur les 7011 décisions qu'elles ont rendues, les commissions administratives de l'OMPI se sont prononcées en faveur des plaignants dans 5842 cas (84%) et les ont déboutés dans 1112 cas (16%).

Au cours de la période qui s'est écoulée entre le lancement de ces services de règlement des litiges selon les principes UDRP en décembre 1999 et le mois d'août 2006, le Centre de l'OMPI a été saisi de 9567 plaintes déposées selon les principes UDRP ou sur la base de ces principes (domaines génériques de premier niveau (gTLD) et domaines de premier niveau qui sont des codes de pays (ccTLD)), portant sur 17 912 noms de domaine distincts qui mettaient en présence des parties provenant de 136 pays.

Ce nombre s'élève à 25 085 si l'on prend en considération les plaintes traitées selon les diverses procédures ad hoc de règlement des litiges survenant au cours d'une phase préliminaire, conçues pour éviter une vague de plaintes liées à des cas de cybersquatting à la suite de l'introduction des nouveaux noms de domaine, à savoir des plaintes relatives aux domaines .info (contestations d'enregistrements préliminaires), .biz (plaintes selon les principes UDRP), .name (plaintes selon les principes UDRP) et .mobi (contestations d'enregistrements préliminaires).

Les principes applicables aux contestations d'enregistrements préliminaires ont permis d'établir des procédures qui offrent aux propriétaires de marques des moyens supplémentaires d'empêcher et de contrecarrer un enregistrement abusif effectué de mauvaise foi de leurs marques comme noms de domaine dans une phase de démarrage déterminée.

Le .com, l'extension la plus litigieuse

La plupart des 9567 plaintes déposées selon les principes UDRP ou sur la base de ces principes concernent des domaines internationaux, le domaine .com représentant environ 79% des noms concernés, suivi par les domaines .net (11%), .org (6%), .info (2%) et .biz, .travel, .aero et .edu (qui représentent ensemble 2%).

4 % de litiges pour les extensions locales

Sur les 9567 plaintes déposées au titre des principes UDRP, 418 litiges portaient sur des noms de domaine enregistrés en tant que ccTLD. Le Centre assure désormais des services de règlement des litiges dans 47 ccTLD tels que .ch (Suisse), .fr (France), .mx (Mexique) et .tv (Tuvalu). Le dernier a avoir été ajouté à cette liste (au début de l'année 2006) est le domaine .es (Espagne).

Les IDN aux rendez-vous

Le Centre propose aussi des services de règlement des litiges pour les enregistrements en caractères autres que latins (n'appartenant pas au code ASCII) tels que les alphabets arabe, chinois, cyrillique ou coréen (noms de domaine "internationalisés") et a reçu jusqu'à présent 60 plaintes en rapport avec ces noms.

Le chiffre de 25 000 noms litigieux est minime par rapport aux 110 millions de noms de domaine existants (à peine 0,2 %). Il ne masque pas les millions de noms litigieux enregistrés pour lesquels les ayants-droits n'agissent pas faute de temps, de moyens ou de politique. Les indications OMPI passent sous silence également l'ensemble des noms récupérés à l'amiable. Rappelons qu'une procédure UDRP coûte 1500 dollars, hors frais des cabinets juridiques, et que les cybersquatteurs proposent souvent une récupération à l'amiable autour de ces tarifs...

R.D.T.I.C
LA REVUE DU DROIT DES TECHNIQUES DE L'INFORMATION ET DE LA COMMUNICATION-
N°57 – OCTOBRE 2006

PROPRIÉTÉS INTELLECTUELLES, DROIT D'AUTEUR

LE DROIT MORAL DE L'AUTEUR SUR LES ŒUVRES NUMÉRIQUES

Par M. Etienne Deshoulieres, LL.M

En France comme en Allemagne, le droit de la propriété littéraire et artistique organise la protection des intérêts moraux de l'auteur.

n France comme en Allemagne, le droit de la propriété littéraire et artistique organise la protection des intérêts moraux de l'auteur. Quatre attributs fondamentaux permettent au créateur de protéger la relation personnelle qu'il entretient avec son œuvre : le droit de divulgation, le droit de paternité, le droit au respect de l'œuvre et le droit de retrait et de repentir. Ces prérogatives sont de nature extrapatrimoniale. Elles ne peuvent donc en principe faire l'objet de convention et s'imposent aux tiers comme aux cocontractants.

Le Code de la propriété intellectuelle et le *Urheberrechtsgesetz* protégeant les œuvres quel que soit leur mode d'expression, les œuvres numériques sont soumises au même régime que les autres créations. Mais la spécificité de ces œuvres soulève des problèmes nouveaux au regard de la protection des intérêts moraux de l'auteur. D'une part, les enjeux du secteur de l'économie numérique sont difficilement conciliables avec la conception personnaliste du droit d'auteur continental. Il peut en effet paraître risqué d'investir dans la production d'œuvres dont l'exploitation peut être remise en cause par les auteurs. Les législateurs français et allemand sont donc intervenus pour atténuer le droit moral là où les intérêts légitimes des investisseurs leur paraissaient devoir être protégés. Les auteurs jouissent ainsi de prérogatives morales limitées sur les œuvres audiovisuelles et les programmes d'ordinateur. D'autre part, le format numérique renouvelle le rapport que le public entretient avec les œuvres. Les techniques de traitement et de communication permettent aux utilisateurs de modifier et de diffuser eux-mêmes les œuvres numérisées. Ces nouvelles possibilités remettent largement en cause l'effectivité du droit moral sur les réseaux numériques.

Mais les auteurs disposent désormais de nouveaux moyens de protection. Les lois de transposition allemande et française de la directive communautaire 2001/29/CE autorisent en effet les mesures techniques de protection et sanctionnent pénalement leur contournement. Les dispositifs de verrouillage des œuvres devraient ainsi permettre aux auteurs de compléter une protection juridique déficiente par une exclusivité technique efficace. Toutefois, il n'est pas certain que les nouvelles solutions de gestion des droits d'auteur s'imposent face aux pratiques des utilisateurs.

Pour plus d'informations, consultez E. Deshoulières, Le droit moral de l'auteur sur les œuvres numériques, Mémoire de master 2 recherche de droit comparé franco-allemand, Sous la direction de M.M. les professeurs Christoph KRAMPE et Louis VOGEL, Université Panthéon-Assas (Paris II) / Humboldt Universität zu Berlin, 2005-2006.

DROIT-TIC .com

R.D.T.I.C

LA REVUE DU DROIT DES TECHNIQUES DE L'INFORMATION ET DE LA COMMUNICATION-
N°57 – OCTOBRE 2006

INFORMATIQUE ET LIBERTÉS, DROIT DE LA COMMUNICATION ET DES TÉLÉCOMMUNICATIONS

L'EFFICACITÉ DU DROIT FACE AUX ABUS D'UTILISATION DES NOUVEAUX OUTILS D'ÉCHANGE : UTOPIE OU RÉALITÉ ?

Par M. Louis-Xavier RANO,
Juriste

Les nouvelles technologies de l'information progressent à grand pas et le droit positif tente d'encadrer cette évolution.

1. La réflexion proposée tente de faire la lumière sur un problème posé à un temps donné. Les nouvelles technologies de l'information progressent à grand pas et le droit positif (constitué notamment par les lois et les décisions des tribunaux) tente d'encadrer cette évolution. Au jour de l'intervention le 9 juin 2006, le projet de loi concernant la protection du droit d'auteur restait en cours de discussion devant les assemblées parlementaires. Le vote de cette loi est intervenu le 01 août 2006.

2. Les outils permettant de communiquer sur l'internet se multiplient, se développent. Les utilisateurs de l'internet ont les moyens techniques offerts par ce dernier pour créer, éditer, publier, communiquer avec le monde entier. Le cadre des frontières terrestres traditionnelles est bouleversé ; les enjeux sont alors modifiés et des problématiques nouvelles voient le jour surtout à propos de la protection des droits et libertés des personnes.

3. C'est la raison pour laquelle je soutiens les activités du CREIS qui favorise la réflexion en faveur de la promotion d'une utilisation cohérente de l'espace internet.

Les caractères principaux des droits fondamentaux sont notamment qu'ils sont opposables aux pouvoirs publics, aux tiers et que l'individu ne peut pas y renoncer. La loi n'a le droit de les limiter que pour protéger un intérêt supérieur ou prioritaire.

4. Ont été proclamés des droits qui touchent directement à la vie des personnes notamment la liberté d'aller et de venir, d'opinions, les droits à la solidarité, à la santé, à la non-discrimination etc. Le législateur, conscient des nouvelles attentes des personnes, construit généralement sa stratégie politique autour de ces grands thèmes et aménage la législation en vigueur.

5. Dans la lignée de mes centres d'intérêt, j'ai réalisé mon mémoire de DEA sur le thème de « *la force du droit à l'oubli* », réflexion qui a été primée par le CREIS le 10 juin 2005. Ce travail a tenté de mettre en exergue la dangerosité de l'utilisation incontrôlée des nouvelles technologies de l'information (développement des moyens de contrôle de l'humain avec notamment l'installation de radars, de fichiers de données à caractère personnel etc.) qui porte atteinte à un ensemble de droits et libertés fondamentales. L'idéal serait la reconnaissance et le respect d'un droit à l'oubli dans notre société et le travail réalisé apporte quelques pistes de réflexions.

6. Je travaille pour le moment au Conseil Départemental de l'Accès au Droit de l'Hérault. Je suis chargé, sous la direction du président du tribunal de grande instance de Montpellier de mettre en place dans tout le département des consultations juridiques gratuites de notaires, huissiers, avocats, juristes à destination d'un public, souvent démuni face à la complexité des règles de droit. L'objectif est bien celui d'aller vers davantage d'égalité entre les personnes. En effet, la loi contre les exclusions et la résolution amiable des conflits votée le 18 décembre 1998 poursuit cet objectif d'aller vers davantage de cohésion sociale et ainsi de favoriser l'égalité entre les personnes. Cela s'insère dans les priorités des pays de développer durablement les conditions de l'humain. (Priorités notamment rassemblées dans un même texte lors du sommet de la Terre en 1992 à Rio sur le thème du développement durable).

7. En parallèle, je suis consultant à la maison de la justice et du droit de Montpellier dans laquelle, cette fois, directement, je fais de l'accès au droit en recevant le public. La difficulté est bien celle de faire preuve de polyvalence étant donné la grande diversité des situations rencontrées. Les personnes attendent une réponse compréhensive, claire, rapide et de qualité. En cas de doute exprimé par le professionnel de droit, celui-ci doit être capable de procéder à une réorientation dans les plus brefs délais. A partir de ces exigences, le juriste se tient informé des textes importants parus et reste proche du milieu institutionnel, associatif en participant à des réunions de réseaux de façon régulière.

8. J'ai proposé au CREIS un sujet d'intervention en fonction du thème de la journée. Nous sommes des utilisateurs de l'internet et témoin des potentialités offertes. Ce thème est : « *L'efficacité du droit face aux abus d'utilisation des nouveaux outils d'échange : utopie*

ou réalité ? ». Nous parlerons d'outils de communication ou plutôt de l'abus d'utilisation de ces nouveaux outils. Le législateur essaie de cadrer l'usage de ces procédés. Osons dire que la législation tente depuis des années de donner un cadre à l'internet ; cadre qui s'appliquerait à ces nouveaux mécanismes.

9. La problématique proposée serait bien celle-ci : le droit permet-il de limiter et sanctionner les abus constatés ? La loi ne cadre t-elle pas trop l'usage de ces outils de sorte que la peur serait celle de trop freiner l'usage ?

Deux concepts vont animer la démarche : celui de liberté et celui de respect.

10. La liberté n'est pas un rêve, une illusion. Elle paraît l'être encore dans certains pays, elle l'était en France sous l'ancien régime, donc à une époque qui n'est pas si lointaine.Cette période a été marquée par la puissance d'une seule personne qui rendait la justice au nom d'un dieu. Des dérives telles l'injustice, l'arbitraire, l'inégalité, sont condamnées par tout un peuple qui se soulève en 1789.La victoire de celui-ci sonne le glas de l'ancien régime. 1789 reste dans les esprits comme une année de fierté, une année rupture, une année provoquant la naissance de la « vraie liberté ».

11. Toutefois, il a fallu attendre près de 50 ans après la révolution de 1789 pour que des hommes et des femmes noirs puissent se lever le matin libres et se coucher le soir libres sans traces sur le corps. En effet, l'abolition française de l'esclavage a été proclamée et il a fallu attendre 1848.

12. Comment définir le concept de liberté ? Le sujet d'intervention n'est absolument pas consacré à cette notion. Cependant il paraît important de donner la définition retenue par les rédacteurs de la déclaration des droits de l'homme et du citoyen (DDHC) votée le 26 août 1789 : dès lors, l'article 4 de la DDHC dispose que : « *La liberté consiste à pouvoir faire tout ce qui ne nuit pas à autrui (…)* ».

La liberté est érigée en principe. L'interdit servirait à protéger cette liberté.

13. Le concept de respect découle de l'association entre liberté et interdit.

La loi garantit à chaque citoyen le respect de ses libertés fondamentales. La liberté fondamentale est celle qui appartient à l'individu, celle qui limite l'action des pouvoirs publics, celle aussi qui influence leur action.

14. Sur l'internet, la loi doit se limiter à donner le cadre permettant l'expression la plus entière des libertés tout en combattant les abus d'utilisation des nouveaux outils d'échange. Pour illustration, la liberté de communication est garantie et la loi du 30 septembre 1986 relative à la liberté de communication le rappelle : « *la communication au public par voie électronique est* ***libre****. L'exercice de cette liberté ne peut être limité que dans la mesure requise d'une part, par le respect de la dignité de la personne humaine, de la liberté et de la propriété d'autrui, du caractère pluraliste de l'expression des courants de pensée et d'opinion et, d'autre part, par la sauvegarde de l'ordre public, par les besoins de la défense nationale, par les exigences de service public, par les contraintes techniques inhérentes aux moyens de communication, ainsi que par la nécessité, pour les services audiovisuels, de développer la production audiovisuelle.* »

15. La démarche qui suit a le souci d'essayer de poser concrètement mais de manière succincte les problèmes rencontrés et d'en rechercher les éléments de solution : dès lors, il s'avère utile dans un premier temps de décrire les enjeux juridiques en terme de protection des droits des personnes du fait de l'utilisation incontrôlée des outils de communication (I) et dans un second, de rechercher les mécanismes légaux qui permettraient d'assurer la protection des droits des personnes. Il paraît opportun d'observer le comportement des juges chargés de faire le lien entre la règle de droit et les abus constatés (II).

Pour plus d'informations se reporter à L-X. RANO, L'efficacité du droit face aux abus d'utilisation des nouveaux outils d'échange : utopie ou réalité ?, intervention du 9 juin 2006 devant le CREIS, Droit-Tic, 2 oct. 2006.
http://www.droit-ntic.com/trav/info.php?id_trav=98

R.D.T.I.C
LA REVUE DU DROIT DES TECHNIQUES DE L'INFORMATION ET DE LA COMMUNICATION-
N°57 – OCTOBRE 2006

DÉCISIONS

CNIL, 28 juin 2006, N° 2006-173 PRONONCANT UNE SANCTION PÉCUNIAIRE À L'ENCONTRE DE LA SCP X

Thèmes
Informatique et libertés, responsabilité
Abstract
CNIL, pouvoir a posteriori, contrôle sur place, entrave, données sensibles, traitements de données à caractère personnel relatives aux infractions, condamnations et mesures de sûreté, collecte déloyale (oui), sanction pécuniaire (oui)
Résumé
Le 17 juillet 2005, la CNIL a été saisie d'une plainte sur les pratiques d'une étude d'huissiers de justice qui avait signifié au requérant une injonction de payer qui, à coté de l'identité du débiteur, comportait la mention « méchant imbécile»
Décision

- La Commission nationale de l'informatique et des libertés, réunie en formation restreinte, sous la présidence de M. Alex Türk, président ;
-

Etant aussi présents M. Guy Rosier, vice-président délégué, M. François Giquel, vice-président, M. Hubert Bouchet, membre, Mlle Anne Debet, membre et M. Bernard Peyrat, membre ;

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 loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, dans sa rédaction antérieure à la loi du 6 août 2004 ;

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 ;

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

Vu la délibération n° 2006-011 adoptée par la CNIL le 24 janvier 2006 ;

Vu la saisine n° 05012064 ;

Vu le rapport de M. Francis Delattre, commissaire, notifié à la SCP X le 10 avril 2006 et les observations en réponse reçues les 14 avril, 21 avril et 2 juin 2006.

Après avoir entendu, lors de la réunion du 28 juin 2006, M. Francis Delattre, commissaire, en son rapport et Mme Pascale Compagnie, commissaire du Gouvernement, en ses observations.

Après avoir entendu, lors de la réunion du 28 juin 2006, les observations orales de Maître X, huissier de justice, celui-ci ayant pris la parole en dernier.

- Constate les faits suivants :

1. Le 17 juillet 2005, la CNIL a été saisie d'une plainte attirant son attention sur les pratiques d'une étude d'huissiers de justice qui avait signifié au requérant, le 21 juin 2005, une injonction de payer qui, à coté de l'identité du débiteur, comportait la mention « méchant imbécile ».
Les 24 et 25 novembre 2005, une délégation de la CNIL s'est rendue dans les locaux de l'étude afin de procéder à une mission de contrôle sur place et vérifier le contenu des fichiers utilisés par cette étude s'agissant, notamment, de l'utilisation de zones « bloc-notes ».

La délégation de la CNIL a procédé le 25 novembre 2005 à une extraction sur support papier des données enregistrées dans la base de données « clients » dénommée « Arche » ainsi que sur cd-rom pour la sauvegarde mensuelle du mois d'août 2005.

Elle a relevé l'existence de nombreux commentaires sur les fiches informatiques des débiteurs sans lien direct avec la finalité du traitement et dénués de toute pertinence ou objectivité. Ces commentaires faisaient, notamment, référence à l'état de santé des personnes, à leurs traits de caractère ou à l'existence de mesures à caractère pénal comme par exemple : « séropositif depuis 23 ans », « ex policier accusé de vol puis relaxé », « déprime », « opération cancer des intestins », « incarcéré Baumettes attend liberté conditionnée », « tentative de suicide », « odieuse », « connasse », etc.
Il est également apparu que des données différentes étaient enregistrées dans la cassette de sauvegarde et dans le listing papier pour les mêmes dossiers. Ainsi par exemple, dans le dossier n° 050119, le listing papier indiquait dans la zone « bloc-notes » : « pensionné COTOREP 50% 599 Eu/Moi * Gros berger allemand ! 0609iiiiii » et, dans la cassette de sauvegarde, dans la même zone « bloc-notes », figurait en plus la mention : « Séropositif depuis 23 ans ». De même, dans le dossier n° 006310, le listing papier indiquait dans la zone « bloc-notes » : « W 2500 CAF 4400 LOYER 800 3 ENFANTS PAS DE PENSION NEE LE 31.05.1955 0622iiiiii » et dans la cassette de sauvegarde, la même zone « bloc-notes » comportait en plus la mention : « CONNASSE ».

Ces faits étaient de nature à constituer un manquement aux obligations découlant de l'article 6-1° de la loi du 6 janvier 1978 modifiée qui dispose qu'un traitement ne peut porter que sur des données à caractère personnel (…) collectées et traitées de manière loyale et licite et de l'article 6-3° de la loi du 6 janvier 1978 modifiée qui dispose qu'un traitement ne peut porter que sur des données à caractère personnel (…) adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et de leurs traitements ultérieurs. Le non-respect de ces obligations est susceptible d'entraîner l'application de l'article 226-18 du code pénal.

De plus, l'article 8 de la loi du 6 janvier 1978 modifiée dispose qu'il est interdit de collecter ou de traiter des données à caractère personnel, en dehors des cas prévus au II de ce même article, 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 de celles-ci.

Par ailleurs, l'article 9-2° de la loi du 6 janvier 1978 modifiée dispose que les traitements de données à caractère personnel relatives aux infractions, condamnations et mesures de sûreté ne peuvent être mis en oeuvre par les auxiliaires de justice que pour les stricts besoins de l'exercice des missions qui leur sont confiées par la loi. A cet égard, les commentaires identifiés étaient manifestement excessifs au regard des missions qui incombent aux huissiers de justice.
Enfin, les commentaires relevaient, pour certains d'entre eux, de l'intimité de la vie privée des clients ou de leurs rapports avec des tiers et pouvaient ainsi relever de l'article 226-22 du code pénal.

Les diligences accomplies par les services de la Commission ont également permis de constater que le fichier utilisé par les huissiers n'avait pas été déclaré à la CNIL et ce malgré l'obligation qui est faite à tout responsable de traitement de déclarer à la CNIL tout traitement de données à caractère personnel et ce préalablement à sa mise en œuvre.

En conséquence, par délibération adoptée le 24 janvier 2006, la CNIL a mis en demeure la SCP X, dans un délai de dix jours à compter de la réception de la délibération, de :

- prendre toute mesure pour procéder à la suppression des mentions visées dans une annexe accompagnant la mise en demeure ainsi que de toute autre mention susceptible de ne pas être conforme aux articles 6-1°, 6-3°, 8 et 9-2° de la loi du 6 janvier 1978 modifiée qui serait enregistrée dans tout traitement de données à caractère personnel mis en œuvre au sein de l'étude et en justifier ;
- justifier les différences qui existaient entre la version papier et la version informatique des extractions qui ont été remises à la délégation de la CNIL ;
- apporter toute garantie, y compris technique, permettant de considérer qu'il n'y avait pas eu, lors du contrôle, de dissimulation de preuve ou de communication à la délégation de la CNIL d'informations ou de documents non conformes au contenu des enregistrements tel qu'il était au moment où les demandes de copies de documents ont été formulées par la délégation de la CNIL ;
- procéder à la déclaration relative au traitement de gestion « clients » mis en œuvre au sein de l'étude d'huissiers.

2. En réponse à la mise en demeure, Maîtres X ont adressé à la CNIL un courrier daté du 10 février 2006.
a. La SCP a d'abord indiqué avoir pris toutes mesures pour procéder à la suppression des mentions visées dans l'annexe adressée par la CNIL et en justifiait par l'envoi des copies d'écran de la zone commentaires des débiteurs concernés. Par ailleurs, la SCP soutenait dans sa réponse qu'en leur qualité d'officiers publics et ministériels, auxiliaires de justice, chargés de signifier les actes de procédure et de mettre à exécution les jugements civils et pénaux, les huissiers de justice étaient fondés à collecter un certain nombre de données à caractère personnel qui peuvent aller au delà des informations liées à l'insolvabilité ou à la solvabilité des personnes.

A cet égard, la SCP soutenait que la collecte de données à caractère personnel concernant l'état de santé ou la situation judiciaire des personnes concernées était justifiée par les besoins des dossiers, pour prévenir des exécutions mal appropriées (moral des débiteurs) ou éviter des troubles à l'ordre public.

Or l'article 8 de la loi du 6 janvier 1978 modifiée prévoit que la collecte de données relatives à l'état de santé des personnes est strictement interdite sauf dérogation prévue par la loi.

Il ressort par ailleurs des dispositions de l'article 9-2° de la loi du 6 janvier 1978 modifiée le 6 août 2004 que les traitements de données à caractère personnel relatives aux infractions, condamnations et mesures de sûreté ne peuvent être mis en oeuvre par les auxiliaires de justice que pour les stricts besoins de l'exercice des missions qui leur sont confiées par la loi. A cet égard, les commentaires identifiés étaient manifestement excessifs au regard des missions qui incombent aux huissiers de

justice (par exemple : « policier accusé de vol puis relaxé », etc.).
Dans ce contexte, force est de constater que la SCP X n'a apporté aucune garantie qu'il avait été procédé, comme la mise en demeure l'exigeait pourtant, à la suppression de toute mention susceptible de ne pas être conforme aux articles 6-1°, 6-3°, 8 et 9-2° de la loi du 6 janvier 1978 modifiée qui serait enregistrée dans tout traitement de données à caractère personnel mis en œuvre au sein de l'étude.

En effet, la SCP X s'est limitée à supprimer certaines des mentions visées dans l'annexe adressée par la CNIL mais n'a mis en œuvre aucune autre mesure permettant de garantir que l'ensemble des fichiers de l'étude avaient fait l'objet pour l'avenir d'un contrôle par les huissiers eux-mêmes (par exemple « balayage » des zones commentaires) et que des mesures de correction seraient, le cas échéant, engagées.

De même, la SCP n'a apporté aucune information sur les mesures qu'il convenait de prendre afin de s'assurer que de tels manquements ne se reproduiraient pas (mesures de sensibilisation du personnel de l'étude, politique régulière de contrôle des zone commentaires par échantillonnage, etc.).

Dans ces conditions la SCP n'a pas respecté la mise en demeure adressée par la CNIL et n'a pas apporté l'ensemble des garanties attendues.

b. La SCP a ensuite fait valoir que la délégation de la CNIL qui s'est présentée le 25 novembre 2005 pour poursuivre sa mission de contrôle avait renoncé à prendre en charge le disque dur de l'étude et que, par conséquent, il n'était pas concevable que les huissiers aient eu l'intention de dissimuler des informations.

Sur ce point, il faut rappeler que les huissiers de justice étaient parfaitement informés de la venue de la délégation le 25 novembre 2005 puisqu'il avait été convenu la veille au soir que la délégation devait revenir chercher le matin suivant les impressions papier commandées ce jour là.

Au demeurant la délégation de la CNIL n'a formulé aucune demande concernant le disque dur de l'étude mais a demandé à avoir copie d'une disquette de sauvegarde mensuelle afin de vérifier que la version imprimée directement par les huissiers était bien conforme aux mentions sur les clients conservées dans une disquette de sauvegarde mensuelle.

Sur ce point, ceci étant consigné dans le procès-verbal de contrôle n° 2005- 083C, un refus a été opposé à la délégation de lui communiquer directement la copie d'une cassette informatique de sauvegarde au motif qu'une copie de la comptabilité de l'étude se trouvait également sur cette cassette et que les informations de nature comptable étaient couvertes par le secret professionnel.
Face au refus réitéré par les huissiers, il a du être procédé à des manipulations informatiques permettant de ne dupliquer sur un support vierge que les informations relatives au fichier « clients », à l'exclusion de la comptabilité. Or la délégation avait formulé une demande d'extraction de l'ensemble des dossiers clients figurant sur la cassette de sauvegarde d'août 2005, y compris les dossiers archivés ; mais cette demande n'a pas été satisfaite au motif que cette manipulation ne pouvait être faite que par le prestataire informatique qui n'était plus joignable. En raison de l'opposition formulée par les huissiers, la délégation n'a donc pas été en mesure de procéder, lors du contrôle, à la copie de l'intégralité des données enregistrées sur les débiteurs.
Dès lors que les circonstances du déroulement du contrôle sur place ne garantissaient pas qu'il n'y ait pas eu de dissimulation de preuve ou de communication à la délégation de la CNIL d'informations ou de documents non conformes au contenu des enregistrements tel qu'il était au moment où les demandes de copies de documents ont été formulées par la délégation de la CNIL.

c. Enfin, concernant le fait que la SCP X n'a pas procédé à la déclaration de son fichier dans le délai imparti dans la mise en demeure, la SCP X a fait valoir que le logiciel qu'elle utilise est agrée par la Chambre Nationale des Huissiers de Justice et que la Chancellerie avait soumis un cahier des charges strict et précis aux sociétés de prestation de services informatiques qui devaient apporter toutes garanties sur la légalité des logiciels et sur leur mode d'utilisation.

Or, en application des dispositions de l'article 3 de la loi du 6 janvier 1978 modifiée, l'obligation de déclaration incombe au responsable de traitement, c'est-à-dire à la personne qui détermine les finalités et les moyens de ce traitement. Ainsi, la SCP X, comme toute autre étude d'huissiers, doit être considérée comme responsable de traitement et aurait dû, par conséquent, respecter les obligations déclaratives découlant du chapitre IV de la loi du 6 janvier 1978 modifiée le 6 août 2004. A cet égard, l'agrément des chambres professionnelles ou du ministère de la Justice, par exemple sur les aspects comptables de certains logiciels, ne constituait en rien une autorisation d'exonération de déclaration.

Il y a donc lieu de constater que la SCP n'a pas respecté la mise en demeure adressée par la CNIL sur ce point.

3. Aux termes des courriers d'observations adressés par la SCP X les 14 avril, 21 avril et 2 juin 2006 et des observations orales formulées par son représentant, lors de la réunion du 28 juin 2006 :

a. La SCP X aurait pris l'initiative de mettre en place un panneau d'affichage dans les locaux de l'étude pour

sensibiliser les collaborateurs à l'usage des zones de commentaires.
Cependant, au regard de la gravité des manquements constatés, la Commission considère que cette mesure est insuffisante. La SCP X n'a mis en œuvre aucune mesure correctrice significative telle qu'une politique régulière de contrôle des zones de commentaires par échantillonnage ou encore des consignes particulières de sensibilisation de son personnel permettant de garantir que les dispositions des articles 6-1° et 6 –3° de la loi du 6 janvier 1978 modifiée le 6 août 2004 seront bien respectées à l'avenir.

La Commission observe plus généralement que la SCP X ne peut valablement soutenir que la collecte de données à caractère personnel concernant l'état de santé ou la situation judiciaire des personnes concernées est justifiée par les besoins de la gestion de ses dossiers, pour prévenir des exécutions mal appropriées (moral des débiteurs) ou éviter des troubles à l'ordre public dans la mesure où les conditions légales requises pour l'exercice d'une telle collecte (articles 8 et 9-2° de la loi du 6 janvier 1978 modifiée le 6 août 2004) ne sont pas réunies en l'espèce.

La Commission constate à cet égard que la SCP X ne s'est pas conformée à la mise en demeure du 24 janvier 2006 qui lui demandait de prendre toute mesure permettant de procéder à la suppression de toute mention figurant dans ses bases de données susceptible de ne pas être conforme aux articles 6-1°, 6-3°, 8 et 9-2° de la loi du 6 janvier 1978 modifiée le 6 août 2004.

b. La SCP X a pris la décision, le 14 avril 2006, de déclarer à la CNIL son traitement de gestion des dossiers. La SCP, qui dans un premier temps avait refusé de faire une telle déclaration à la CNIL, a néanmoins fait remarquer qu'une déclaration avait déjà été effectuée en 1986, il y a 20 ans, par un autre huissier de justice domicilié à La Ciotat dont l'activité à été rachetée depuis ; la SCP a estimé que cette première déclaration était suffisante et la CNIL aurait du s'en satisfaire.

La Commission rappelle qu'aux termes des dispositions du chapitre IV de la loi du 6 janvier 1978 modifiée, tout responsable de traitement doit procéder à la déclaration des traitements qu'il met en œuvre et doit si nécessaire les mettre à jour. En l'espèce, la déclaration mentionnée n° 149824 du 8 octobre 1986 ne visait en aucune manière l'activité de la SCP X (nom du responsable de traitement, adresse et code SIREN différents).

La Commission observe que la SCP X n'a pas souhaité se conformer à la mise en demeure qui lui était faite de déclarer son traitement et a attendu plus de trois mois avant de décider de satisfaire à la réglementation. La Commission considère par conséquent que la SCP X ne s'est pas conformée à la mise en demeure du 24 janvier 2006 dans le délai qui lui était imparti.
c. La SCP X indique enfin qu'elle est bien soumise au secret professionnel et qu'elle était donc fondée à refuser la demande formulée par la CNIL de la copie d'une cassette informatique de sauvegarde des données sur les débiteurs au motif de la présence, sur cette cassette, de la comptabilité de l'étude.

Il ressort des dispositions de la loi du 6 janvier 1978 modifiée le 6 août 2004 que les membres et les agents habilités de la CNIL peuvent, lors d'un contrôle, demander communication de tous documents nécessaires à l'accomplissement de leur mission, quel qu'en soit le support, et en prendre copie ; qu'ils peuvent accéder aux programmes informatiques et aux données, ainsi qu'en demander la transcription par tout traitement approprié dans des documents directement utilisables pour les besoins du contrôle.

Par ailleurs, en application des dispositions de la loi précitée, les ministres, autorités publiques, dirigeants d'entreprises publiques ou privées, responsables de groupements divers et plus généralement les détenteurs ou utilisateurs de traitements ou de fichiers de données à caractère personnel ne peuvent s'opposer à l'action de la commission ou de ses membres et doivent au contraire prendre toutes mesures utiles afin de faciliter sa tâche. Le non respect de cette disposition est susceptible de constituer un délit d'entrave.

Il ressort par ailleurs des dispositions de l'article 69 du décret n° 2005-1309 du 20 octobre 2005 que lorsqu'une personne interrogée dans le cadre des vérifications faites par la commission oppose le secret professionnel, il doit alors être fait mention des dispositions législatives ou réglementaires auxquelles se réfère la personne interrogée ainsi que la nature des données qu'elle estime couvertes par ces dispositions.

Interrogée sur le fondement juridique du secret professionnel opposé aux agents de la CNIL, la SCP X a invoqué auprès membres de la formation restreinte, lors de la réunion du 28 juin 2006, l'existence de l'article 226-13 du code pénal.

La Commission observe d'une part que la seule référence aux dispositions du code pénal n'est pas suffisante à démontrer de l'existence, au profit de la SCP X, d'une disposition législative ou réglementaire lui permettant de s'opposer aux demandes formulées par la CNIL dans l'exercice de ses missions visées à l'article 44 de la loi du 6 janvier 1978 modifiée le 6 août 2004.

La Commission observe d'autre part que l'existence éventuelle du secret professionnel ne saurait en aucune manière protéger les données relatives à la comptabilité de l'étude. Par conséquent, la nature des données que la SCP X estimait couvertes par le secret professionnel, tel

que cela ressort notamment du procès verbal de contrôle n° 2005- 083C, n'était manifestement pas à même de fonder valablement le refus de communiquer aux agents de la CNIL les informations qu'ils demandaient dans l'exercice de leurs missions.

Il convient de rappeler que ce refus a eu pour conséquence d'empêcher la délégation de la CNIL de procéder à un contrôle exhaustif du contenu des fichiers utilisés par la SCP X.

La Commission relève par conséquent que la SCP X ne s'est pas conformée à la mise en demeure du 24 janvier 2006 puisqu'elle n'a en aucune manière apporté des garanties permettant de considérer qu'il n'y avait pas eu, lors du contrôle, de dissimulation de preuve ou de communication à la délégation de la CNIL d'informations ou de documents non conformes au contenu des enregistrements tel qu'il était au moment où les demandes de copies de documents ont été formulées par la délégation de la CNIL.

4. Il ressort de l'ensemble de ce qui précède que :

- La SCP X ne s'est pas conformée à la mise en demeure du 24 janvier 2006 qui lui demandait de prendre toute mesure permettant de procéder à la suppression de toute mention susceptible de ne pas être conforme aux articles 6-1°, 6-3°, 8 et 9-2° de la loi du 6 janvier 1978 modifiée.

- la SCP X ne s'est pas conformée à la mise en demeure du 24 janvier 2006 de procéder à la déclaration de ses traitements dans le délai qui lui était imparti.

- la SCP X ne s'est pas conformée à la mise en demeure du 24 janvier 2006 puisqu'elle n'a en aucune manière apporté des garanties permettant de considérer qu'il n'y avait pas eu, lors du contrôle, de dissimulation de preuve ou de communication à la délégation de la CNIL d'informations ou de documents non conformes au contenu des enregistrements tel qu'il était au moment où les demandes de copies de documents ont été formulées par la délégation de la CNIL.

-

La Commission relève que l'ensemble de ces faits constituent un manquement aux dispositions de la loi du 6 janvier 1978 modifiée le 6 août 2004 visées dans la présente délibération.

En conséquence, décide de faire application des dispositions des articles 45 et 47 de la loi du 6 janvier 1978 modifiée le 6 août 2004 et de prononcer, compte-tenu de la gravité des manquements commis, une sanction pécuniaire à l'encontre de la SCP X, sise à X, d'un montant de 5000 euros.
Le président, Alex Türk

Référence : CNIL, 28 juin 2006, *N° 2006-173 PRONONCANT UNE SANCTION PÉCUNIAIRE À L'ENCONTRE DE LA SCP X*, DROIT-TIC
http://www.droit-tic.com/juris/aff.php?id_juris=82

R.D.T.I.C
LA REVUE DU DROIT DES TECHNIQUES DE L'INFORMATION ET DE LA COMMUNICATION-
N°57 – OCTOBRE 2006

CNIL, 05 octobre 2006, N°2006-228 PORTANT RECOMMANDATION RELATIVE À LA MISE EN ŒUVRE PAR LES PARTIS OU GROUPEMENTS À CARACTÈRE POLITIQUE, ÉLUS OU CANDIDATS À DES FONCTIONS ÉLECTIVES DE FICHIERS DANS LE CADRE DE LEURS ACTIVITÉS POLITIQUES

Thèmes
Informatique et libertés, Pourriel, spam, courriel, vie privée
Abstract
prospection politique, obligation, responsabilité
Résumé
Au regard de la loi, les partis ou groupements à caractère politique, élus et candidats sont responsables des traitements qu'ils mettent en œuvre et ce, quand bien même ils feraient appel à des prestataires extérieurs.
Décision

- 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 directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement de données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques ;

Vu le code des postes et des communications électroniques, et notamment son article L.34-5 ;

Vu le code électoral, et notamment ses articles L. 28 et R. 16 ;

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° 88-227 du 11 mars 1988 modifiée relative à la transparence financière de la vie politique ;

Vu la loi n° 90-55 du 15 janvier 1990 modifiée relative à la limitation des dépenses électorales et à la clarification du financement des activités politiques ;

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

Après avoir entendu Mme Isabelle Falque-Pierrotin, commissaire, en son rapport et Mme Pascale Compagnie, commissaire du Gouvernement, en ses observations ;

- Formule les observations suivantes :

Les partis ou groupements à caractère politique, élus ou candidats à des fonctions électives recourent à des traitements de données à caractère personnel pour gérer leurs fichiers de membres, de sympathisants ou de personnes s'étant mises en relation avec eux, organiser des élections internes ou réaliser des opérations de communication politique.

Compte tenu du caractère sensible des données traitées, la Commission estime nécessaire de préciser les modalités selon lesquelles les principes de protection des données à caractère personnel doivent s'appliquer à ces traitements afin de garantir pleinement le respect des droits et libertés des personnes.

Tel est l'objet de la présente recommandation, qui abroge et remplace la délibération du 3 décembre 1996.

- Rappelle :

Au regard de la loi, les partis ou groupements à caractère politique, élus et candidats sont responsables des traitements qu'ils mettent en œuvre et ce, quand bien même ils feraient appel à des prestataires extérieurs.
A ce titre, ils doivent veiller au respect de l'ensemble des dispositions de la loi "informatique et libertés" du 6 janvier 1978 modifiée en août 2004 et, en particulier, celles prévues à l'article 8 qui garantit une protection spécifique au traitement des données relatives aux opinions politiques des personnes.

- Recommande :

- I. Sur la gestion des fichiers internes mis en œuvre par les élus, candidats, partis ou groupements à caractère politique,

- Conformément à l'article 8 de la loi du 6 janvier 1978 modifiée, les partis ou groupements à caractère politique qui mettent en œuvre des traitements relatifs à leurs membres ou aux personnes qui entretiennent avec eux des contacts réguliers dans le cadre de leur activité politique (par exemple, les personnes qui versent des fonds, qui soutiennent de manière régulière l'action du parti ou de l'organisme politique concerné ou qui sont abonnées à une

lettre d'information éditée par le parti ou le groupement à caractère politique) n'ont pas à effectuer de déclaration auprès de la CNIL ni à recueillir le consentement des personnes dont les données sont traitées.

- En revanche, les traitements mis en œuvre par les élus ou les candidats et les traitements mis en œuvre par les partis ou groupements à caractère politique qui comprennent des données relatives aux personnes s'étant occasionnellement mises en relation avec eux (à l'occasion de l'envoi d'une pétition, d'une demande de documentation ou d'une visite sur un « blog » par exemple) doivent être déclarés à la CNIL. Ces traitements peuvent être déclarés en référence à la norme simplifiée n° 34 adoptée par la Commission.

Lorsque ces traitements sont susceptibles de faire apparaître les opinions politiques, réelles ou supposées, des personnes, la loi impose le recueil de leur consentement écrit.

L'ensemble des traitements mis en œuvre par un parti, un groupement à caractère politique, un élu ou un candidat doit respecter les conditions suivantes en manière d'information des personnes, d'exercice de droits des personnes et de confidentialité des informations traitées.

- A. l'information des personnes lors de la collecte de leurs données

Les personnes doivent être informées, au moment de la collecte de leurs données :

- de l'identité de celui qui procède à cette collecte : s'agit-il d'un parti politique, d'un comité de soutien extérieur au parti, d'un candidat, d'un groupe de sympathisants ? ;
- de la ou des finalité(s) de cette collecte : les données collectées sont-elles utilisées à des fins de gestion de l'adhésion et des cotisations, pour l'envoi de journaux et autres documents de communication politique ? Les données collectées sont-elles destinées à être diffusées sur un site web de soutien à un candidat ? etc. ;
- du caractère obligatoire ou facultatif de leurs réponses et des conséquences en cas de défaut de réponse ;
- des destinataires des informations collectées : les données sont-elles uniquement destinées à la fédération locale, sont-elles transmises au siège du parti ?
- des modalités selon lesquelles elles peuvent exercer leur droit d'accès, de rectification et de radiation auprès du service ou de la personne désignée pour répondre à ces demandes.

Ces mentions doivent figurer sur les bulletins d'adhésion et sur l'ensemble des supports (tracts, pages web, etc.) permettant un recueil de données à caractère personnel.
En outre, les sites web peuvent utilement comporter une rubrique « informatique et libertés/ protection des données personnelles » accessible dès la page d'accueil.

- B. les droits des personnes dont les données sont traitées

Les personnes doivent pouvoir exercer facilement, et dans des délais rapides, les droits qui leur sont reconnus par la loi. En particulier, le droit :

- d'obtenir, en justifiant de leur identité, communication et copie de l'ensemble des informations les concernant, ainsi que celui de se faire communiquer l'origine des ces informations ;
- d'exiger que les informations les concernant qui sont inexactes, incomplètes, équivoques ou périmées soient rectifiées, complétées, mises à jour ou effacées ;
- de s'opposer, à tout moment, à la conservation par l'élu, le candidat, le parti ou le groupement politique des données à caractère personnel les concernant.

L'exercice de ces droits doit être facilité par la mise en place d'une adresse postale ou d'une adresse de courrier électronique spécifiquement dédiée à cet effet dont l'existence aura été portée clairement à la connaissance des personnes intéressées sur les différents supports de collecte des données.

Enfin, les données recueillies ne peuvent être cédées à des tiers, sauf accord écrit des personnes concernées.

- C. Les conditions de sécurité, d'accès et de communication des données traitées par les partis ou groupements à caractère politique, les élus ou les candidats

La loi impose une obligation de sécurité qui doit conduire le responsable du traitement à prendre toutes précautions utiles pour empêcher que les données soient déformées, endommagées ou que des tiers non autorisés y aient accès.
La Commission appelle l'attention des élus, candidats, partis ou groupements à caractère politique sur le respect de cette obligation, en particulier au regard de la nature sensible des données collectées.

- Ainsi, la Commission recommande que l'accès aux fichiers, et la communication éventuelle des listes des adhérents, soient réservés aux seuls responsables du parti. En effet, eux seuls peuvent, dans le cadre de leur fonction au plan national ou local, légitimement y prétendre, aux côtés des personnels administratifs habilités à

gérer ces traitements.

Les conditions de ces accès devraient être précisées dans les statuts du parti ou du groupement à caractère politique.

- Les accès individuels aux traitements devraient être garantis, par exemple, par l'attribution d'un identifiant et d'un mot de passe individuels, régulièrement renouvelés, ou par tout autre moyen d'authentification.

- La transmission, à des fins de communication politique, de la liste des adhérents à un candidat à une élection interne à un parti politique est possible sous réserve que ce dernier s'engage à ne pas en faire un usage autre. En cas d'organisation d'une élection interne par vote électronique, la Commission préconise le respect des dispositions de sa recommandation en date du 1er juillet 2003.

- L'utilisation de courriers électroniques aux fins de communication et, de façon générale, du réseau internet pour transmettre des fichiers doit s'accompagner des mesures de sécurité adéquates telles que le masquage des adresses de courriers électroniques utilisées ou encore le recours à des moyens de cryptage lors de la transmission du fichier.

II. Sur l'organisation d'opérations de communication politique,

- A. L'utilisation de fichiers constitués par le candidat ou le parti politique lui-même,

Un parti, un groupement à caractère politique, un élu ou un candidat peut utiliser, à des fins de communication politique, les fichiers qu'il détient dès lors que les données ont été collectées en conformité avec les principes rappelés ci-dessus et sous réserve de permettre aux personnes démarchées de s'opposer à tout moment à la réception de nouveaux messages et de se faire radier, le cas échéant, du fichier utilisé.

- B. L'interdiction d'utiliser les fichiers des administrations ou des collectivités locales,

Les fichiers mis en œuvre dans les administrations et les collectivités locales ne peuvent être utilisés que pour les seules finalités pour lesquelles ils ont été constitués dans le cadre des missions de service public qui leur sont imparties. Toute autre utilisation est susceptible de constituer un détournement de finalité, constitutive d'une infraction pénale.
Dès lors, l'utilisation de ces fichiers à des fins de communication politique ne peut être admise.

Ainsi, à titre d'exemple, les registres d'état civil, les fichiers de taxes et redevances, les fichiers d'aide sociale, les fichiers de parents d'élèves, les adresses de courrier électronique collectées à partir d'un site web institutionnel et, d'une façon générale, les fichiers d'administrés et d'usagers ne peuvent en aucun cas être utilisés à des fins de communication politique.

- C. L'utilisation de la liste électorale,

Aux termes de l'article L. 28 du code électoral, tout électeur, tout candidat et tout parti ou groupement politique peut prendre communication et copie de la liste électorale auprès des communes concernées, à la condition de ne pas en faire un usage commercial.
Cette disposition n'interdit pas aux élus, candidats ainsi qu'aux partis et groupements politiques, d'utiliser les informations issues des listes électorales à des fins de recherche de moyens de financement.

Il est possible d'opérer, à partir des listes électorales obtenues, des extractions en fonction de l'âge ou du bureau de vote de rattachement des électeurs afin d'effectuer une opération de communication politique ciblée.

En revanche, la Commission estime qu'un traitement consistant à opérer des tris sur la base de la consonance du nom des électeurs, sur leur département ou leur lieu de naissance afin de s'adresser à eux en raison de leur appartenance, réelle ou supposée, à telle communauté ethnique ou religieuse, ne constitue pas, au regard des articles 6 et 8 de la loi, une collecte loyale et licite de données. Un tel traitement doit donc être proscrit car comportant un risque de sélection et de discrimination susceptible de porter atteinte aux droits et libertés des personnes.

La Commission recommande que tout courrier adressé à un électeur à partir de la liste électorale indique l'origine des informations utilisées pour le lui faire parvenir.

- D. L'utilisation des fichiers commerciaux,

- Seuls les fichiers loués ou cédés à des fins de prospection commerciale (fichiers de clients ou de prospects) peuvent être utilisés par un candidat, un élu ou un parti politique à des fins de communication politique.
- Ainsi, les fichiers de gestion interne (par exemple, les fichiers de gestion et de paie du personnel) ne peuvent être utilisés à des fins de communication politique.
- L'élu, le candidat ou le parti ou le groupement à caractère politique est responsable du traitement mis en œuvre dans le cadre d'une opération de prospection politique, quand bien même l'organisation de cette campagne ne le conduit pas à traiter directement les données à

caractère personnel des personnes démarchées, c'est-à-dire lorsqu'il fait appel aux services de sociétés extérieures qui gèrent elles-mêmes l'organisation et la réalisation technique de l'opération de prospection.

A ce titre, il doit procéder à la déclaration du traitement à la CNIL et s'assurer, notamment par l'insertion de clauses spécifiques dans le contrat de location du fichier dont l'utilisation est envisagée, que les personnes ont été informées de l'utilisation à des fins de prospection politique de leurs données et des droits qui leur sont ouverts au titre de la loi "informatique et libertés".

Une sélection des personnes à démarcher, notamment sur la base de leur centre d'intérêt (par exemple, la politique), de leur âge ou de leur résidence géographique est possible à la condition qu'elle ne se base pas sur la consonance des noms des personnes ou sur leur lieu de naissance et qu'elle ne fasse pas apparaître, directement ou indirectement, les origines raciales, ou ethniques ou les opinions politiques, réelles ou supposées, des personnes concernées.

- La particularité des opérations de prospection politique conduit la Commission à recommander une information particulière des personnes dont les données sont traitées, d'une part, lors de la collecte de leurs données, d'autre part, lors de la réception du message.

- 1. la nécessité d'une information claire et transparente des personnes lors de la collecte de leurs données

La Commission recommande que les personnes soient averties, lors du recueil de leurs données par le prestataire détenteur du fichier dont l'utilisation est envisagée, de la possible utilisation de leurs données à des fins de prospection politique.

- concernant l'organisation d'opérations de prospection par voie postale ou téléphonique,
  Les personnes doivent, en outre, être averties de leur droit de s'opposer à cette utilisation et à la transmission à des tiers de leurs données – ici, le parti, le groupement à caractère politique, le candidat ou l'élu – par un moyen simple et immédiat, une case à cocher par exemple.
- concernant l'organisation d'opérations de prospection par voie électronique,

  La loi pour la confiance dans l'économie numérique du 21 juin 2004 a posé le principe du consentement préalable des personnes concernant la réception de messages de « prospection directe », entendu au sens de commerciale, fournis notamment au moyen de courriers électroniques, mais n'a pas abordé le cas de la prospection politique.

  Face au silence de la loi, la Commission estime que ce régime devrait s'appliquer aux opérations de prospection politique opérées par voie électronique et, dès lors, appelle l'attention du Gouvernement sur l'intérêt qui s'attacherait à ce qu'une disposition législative vienne préciser le régime juridique applicable aux opérations de prospection politique opérées par voie électronique.

  La Commission estime dès à présent que les opérations de prospection politiques opérées par courrier électronique devraient n'utiliser que des bases de données de personnes ayant exprimé leur consentement à être démarchées, dits fichiers « opt-in ». (exemple de recueil de consentement par une case à cocher : « Oui, j'accepte de recevoir par e-mail des sollicitations de vos partenaires commerciaux, d'associations ou de groupements à caractère politique »).

  Prenant acte du fait que les personnes dont les adresses de courrier électronique sont aujourd'hui contenues dans les fichiers de prospection commerciale n'ont pas été informées de la possible utilisation de leurs données à des fins de prospection politique, la Commission recommande que les gestionnaires de bases de données souhaitant proposer la location de leur base à des fins de prospection politique adressent un courrier électronique à chacune des personnes présentes dans leur base pour les informer que leur adresse électronique est dorénavant susceptible d'être utilisée à des fins de prospection politique et de la faculté qu'elles ont de s'y opposer.

- 2. la nécessité de renforcer l'information des personnes lors de la réception d'un message de prospection politique

La Commission préconise que le message envoyé aux personnes sollicitées, quel que soit le support utilisé, précise de façon claire et visible :

- l'origine du ou des fichiers utilisés ou du programme de fidélisation auquel elles se seraient inscrites (par exemple : « Vous recevez cet e-mail/ ce courrier parce que vous vous êtes inscrit auprès de …. Si vous ne souhaitez plus recevoir de messages de sa part, cliquez ici/ écrivez à l'adresse ci-dessous ») ;
- le fait que le candidat, l'élu ou le parti à l'origine de la campagne ne dispose pas de l'adresse

utilisée mais a eu recours à un prestataire extérieur (par exemple : « Ce message vous a été envoyé par un prestataire pour le compte de notre parti qui n'a pas connaissance de votre adresse ») ;

- du droit de s'opposer, à tout moment, à recevoir de tels messages. L'exercice de ce droit doit permettre à l'internaute de ne plus recevoir de message à vocation de prospection politique du fichier à partir duquel ses coordonnées électroniques ont été utilisées.

- 3. la gestion des radiations exprimées par les personnes

Un parti, un groupement à caractère politique, un élu ou un candidat ne peut traiter lui-même dans un fichier (type « liste rouge ») les données des personnes ne souhaitant plus être démarchées. En effet, la constitution d'un tel fichier pourrait révéler, directement ou indirectement, les opinions politiques des personnes qui y sont inscrites. Il revient donc aux prestataires de gérer le fichier des oppositions exprimées par les personnes, en évitant toute indication susceptible de révéler indirectement les opinions politiques des personnes, à savoir la campagne à l'origine de la demande de désinscription.

- 4. l'utilisation d'autres moyens de communications électroniques

Au regard du caractère particulièrement intrusif de la prospection opérée par télécopieurs ou par automates d'appel, la Commission recommande que les candidats, élus ou partis et groupements à caractère politique s'abstiennent d'utiliser ces moyens de communication pour effectuer une opération de prospection politique.
La Commission relève que le format actuel des messages qui peuvent être envoyés sur les téléphones portables (SMS) ne permet généralement pas de fournir aux personnes démarchées les informations nécessaires dans le cadre d'une opération de prospection politique. En conséquence, elle préconise de ne pas utiliser ce moyen de communication afin de réaliser des opérations de communication politique.

- III. Sur l'organisation d'opérations de parrainage,

Les partis, groupements à caractère politique, élus ou candidats peuvent vouloir organiser des opérations de parrainage leur permettant de s'adresser directement à une personne dont les données leur auront été communiquées par un tiers.
Les opérations de parrainage constituant un mode de collecte indirecte de données, la Commission recommande qu'il soit adressé à la personne ainsi parrainée un seul et unique message l'informant de l'identité de la personne lui ayant transmis ses coordonnées (le parrain) et l'invitant à entrer en contact avec le parti, le groupement à caractère politique, l'élu ou le candidat à l'origine du message et, qu'à défaut, les coordonnées soient effacées à l'issue de cette opération (exemple : « Votre adresse nous a été transmise par M. X. Elle n'est pas conservée et n'a été utilisée que pour vous faire parvenir ce message vous invitant à rentrer en contact avec nous en nous contactant à l'adresse suivante / par l'intermédiaire de notre site web).

Le président, Alex Türk

Disponible sur le site de la cnil : http://www.cnil.fr/index.php?id=2133

Référence : CNIL, 05 octobre 2006, *N°2006-228 PORTANT RECOMMANDATION RELATIVE À LA MISE EN ŒUVRE PAR LES PARTIS OU GROUPEMENTS À CARACTÈRE POLITIQUE, ÉLUS OU CANDIDATS À DES FONCTIONS ÉLECTIVES DE FICHIERS DANS LE CADRE DE LEURS ACTIVITÉS POLITIQUES*, DROIT-TIC
http://www.droit-tic.com/juris/aff.php?id_juris=81

R.D.T.I.C
LA REVUE DU DROIT DES TECHNIQUES DE L'INFORMATION ET DE LA COMMUNICATION-
N°57 – OCTOBRE 2006

TEXTES OFFICIELS

Arrêté du 26 septembre 2006 portant définition des normes techniques des systèmes de vidéosurveillance

J.O n° 233 du 7 octobre 2006 page 14859, texte n° 4.

NOR: INTC0600806A

Le ministre d'Etat, ministre de l'intérieur et de l'aménagement du territoire,

Vu la loi n° 95-73 du 21 janvier 1995 d'orientation et de programmation modifiée relative à la sécurité ;

Vu le décret n° 96-926 du 17 octobre 1996 relatif à la vidéosurveillance pris pour l'application de l'article 10 de la loi n° 95-73 du 21 janvier 1995 d'orientation et de programmation relative à la sécurité, modifié par le décret n° 2002-814 du 3 mai 2002 pris pour l'application de l'article 21 de la loi n° 2000-321 du 12 avril 2000 et relatif aux délais faisant naître une décision implicite de rejet et par le décret n° 2006-665 du 7 juin 2006 relatif à la réduction du nombre et à la simplification de la composition de diverses commissions administratives,

Arrête :

Article 1

Les caméras sont réglées, équipées et connectées au système de visualisation et, le cas échéant, au système de stockage, de façon que les images restituées lors de la visualisation en temps réel ou en temps différé permettent de répondre aux finalités pour lesquelles le système de vidéosurveillance a été autorisé.

Les caméras présentent les caractéristiques techniques adaptées aux conditions d'illumination du lieu vidéosurveillé.

Les réseaux sur lesquels transitent les flux vidéo offrent une bande passante compatible avec les débits nécessaires à la transmission d'images de qualité suffisante pour répondre aux finalités pour lesquelles le système de vidéosurveillance a été autorisé.

Les réseaux sur lesquels transitent les flux vidéo prennent en compte la sécurité de ces derniers, garantissant leur disponibilité, leur confidentialité et leur intégrité.

Article 2

Le stockage des flux vidéo est réalisé sur support numérique pour les systèmes de vidéosurveillance comportant huit caméras ou plus. Ce stockage peut également être réalisé sur un autre type de support. Le stockage des flux vidéo est réalisé sur support analogique ou numérique pour les systèmes de vidéosurveillance comportant moins de huit caméras.

Tout flux vidéo enregistré numériquement est stocké avec des informations permettant de déterminer à tout moment de la séquence vidéo sa date, son heure et l'emplacement de la caméra.

Pour les systèmes à enregistrement analogique des flux vidéo, un dispositif permet de déterminer à tout moment la date, l'heure et l'emplacement de la caméra correspondant aux images enregistrées.

L'enregistrement numérique garantit l'intégrité des flux vidéo et des données associées relatives à la date, à l'heure et à l'emplacement de la caméra.

Les flux vidéo stockés issus des caméras qui, compte tenu de leur positionnement et de leur orientation, fonctionnent principalement en plan étroit, à l'exclusion de celles de régulation du trafic routier, ont un format d'image supérieur ou égal à 704 576 pixels. Ce format pourra être inférieur si le système permet l'extraction de vignettes de visage d'une résolution minimum de 90 60 pixels.

Les autres flux vidéo stockés ont un format d'image supérieur ou égal à 352 288 pixels.

Une fréquence minimale de douze images par seconde est requise pour l'enregistrement des flux vidéo issus de caméras installées pour une des finalités mentionnées au II de l'article 10 de la loi du 21 janvier 1995 susvisée, à l'exclusion de celles de régulation du trafic routier, et qui, compte tenu de leur positionnement et de leur orientation, fonctionnent principalement en plan étroit et filment principalement des flux d'individus en déplacement rapide.

Pour l'enregistrement des autres flux vidéo, une fréquence minimale de six images par seconde est requise.

Le système de stockage utilisé est associé à un journal qui conserve la trace de l'ensemble des actions effectuées sur les flux vidéo.

Pour les systèmes numériques, ce journal est généré automatiquement sous forme électronique.

Article 3

Les flux vidéo sont exportés sans dégradation de la qualité :

Pour les systèmes de vidéosurveillance utilisant la technologie analogique, un dispositif détermine la liste des flux exportés indiquant la date et l'heure des images filmées, leur durée, l'identifiant des caméras concernées, la date et l'heure de l'exportation, l'identité de la personne ayant réalisé l'exportation.

Pour les systèmes de vidéosurveillance utilisant la technologie numérique, un journal électronique des exportations, comportant les informations citées à l'alinéa précédent, est généré automatiquement.

Le système d'enregistrement reste en fonctionnement lors de ces opérations d'exportation.

Le support physique d'exportation est un support numérique non réinscriptible et à accès direct, compatible avec le volume de données à exporter. Dans le cas de volumes importants de données à exporter, des disques durs utilisant une connectique standard pourront être utilisés. Pour les systèmes numériques de vidéosurveillance, un logiciel permettant l'exploitation des images est fourni sur support numérique, disjoint du support des données.

Le logiciel permet :

1° La lecture des flux vidéo sans dégradation de la qualité de l'image ;

2° La lecture des flux vidéo en accéléré, en arrière, au ralenti ;

3° La lecture image par image des flux vidéo, l'arrêt sur une image, la sauvegarde d'une image et d'une séquence, dans un format standard sans perte d'information ;

4° L'affichage sur l'écran de l'identifiant de la caméra, de la date et de l'heure de l'enregistrement ;

5° La recherche par caméra, date et heure.

Article 4

Le directeur général de la police nationale et le directeur général de la gendarmerie nationale sont chargés, chacun en ce qui le concerne, de l'exécution du présent arrêté, qui sera publié au Journal officiel de la République française.

Fait à Paris, le 26 septembre 2006.

Nicolas Sarkozy

© J. Le Clainche