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

ANALYSES

■ QUAND DROIT D'AUTEUR RIME AVEC OFFRES SANS SCRUPULES
Par Melle Astrid Stumpf, Juriste

■ RAISON SOCIALE, MARQUE ET NOM DE DOMAINE
Par Mme Marie Roulleaux-Dugage, Chef du service de l'Opposition à l'INPI

■ LA SÉCURITÉ DES SITES INTERNET ET DES SYSTÈMES D'INFORMATIONS : QUELLES RESPONSABILITÉS ?
Par Nicolas Samarcq, juriste TIC

■ LIMITES DE LA SPHÈRE DE VIE PRIVÉE ÉLECTRONIQUE DES SALARIÉS
Par M. Raphaël Rault, Juriste TIC - BRM Avocats

■ LA (RE)NÉGOCIATION DES CONTRATS DE COMMUNICATIONS ÉLECTRONIQUES
Par Me. Anne-Katel Martineau, Avocat - SCP COURTOIS LEBEL et Me. Arnaud Tessalonikos Avocat Counsel - SCP COURTOIS LEBEL

■ QUAND REPRODUCTION À L'IDENTIQUE NE RIME PAS AVEC CONTREFACON
Par M.Benjamin Vitasse, Juriste - Consultant noms de domaine

DELIBERATIONS CNIL

■ Délibération n° 2005-188 du 8 septembre 2005 portant avis sur le projet de décret en Conseil d'Etat pris pour l'application de l'article 26 (II) de la loi du 6 janvier 1978 modifiée et portant création du système d'information judiciaire JUDEX

TEXTE OFFICIEL

■ Décret n° 2006-1405 du 17 novembre 2006 modifiant le décret n° 64-754 du 25 juillet 1964 relatif à l'organisation du ministère de la justice et

JURISPRUDENCES

■ CA de Paris, 14ème chambre, section B, 26 novembre 2006, SA TISCALI, AFA, FRANCE TELECOM ET ALII / UEJF, J'ACCUSE, SOS RACISME ET ALII (Contenus et comportements illicites, responsabilité)

■ C. Cass., Ch. soc., 18 octobre 2006, J. LE F⊗⊗⊗⊗ / SARL TECHNI-SOFT (Droit social, informatique et libertés)

DROIT-TIC .com

© Julien Le Clainche

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

- 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°58 – NOVEMBRE 2006

ANALYSES

■ QUAND DROIT D'AUTEUR RIME AVEC OFFRES SANS SCRUPULES

Par Melle Astrid Stumpf, Juriste

■ RAISON SOCIALE, MARQUE ET NOM DE DOMAINE

Par Mme Marie Roulleaux-Dugage, Chef du service de l'Opposition à l'INPI

■ LA SÉCURITÉ DES SITES INTERNET ET DES SYSTÈMES D'INFORMATIONS : QUELLES RESPONSABILITÉS ?

Par Nicolas Samarcq, juriste TIC

■ LIMITES DE LA SPHÈRE DE VIE PRIVÉE ÉLECTRONIQUE DES SALARIÉS

Par M. Raphaël Rault, Juriste TIC - BRM Avocats

■ LA (RE)NÉGOCIATION DES CONTRATS DE COMMUNICATIONS ÉLECTRONIQUES

Par Me. Anne-Katel Martineau, Avocat - SCP COURTOIS LEBEL et Me. Arnaud Tessalonikos Avocat Counsel - SCP COURTOIS LEBEL

■ QUAND REPRODUCTION À L'IDENTIQUE NE RIME PAS AVEC CONTREFACON

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

DÉCISIONS

■ CA de Paris, 14ème chambre, section B, 26 novembre 2006, SA TISCALI, AFA, FRANCE TELECOM ET ALII / UEJF, J'ACCUSE, SOS RACISME ET ALII (Contenus et comportements illicites, responsabilité)

■ C. Cass., Ch. soc., 18 octobre 2006, J. LE F⊗⊗⊗⊗ / SARL TECHNI-SOFT (Droit social, informatique et libertés)

DÉCRET

■ Décret n° 2006-1405 du 17 novembre 2006 modifiant le décret n° 64-754 du 25 juillet 1964 relatif à l'organisation du ministère de la justice et instituant une délégation aux interceptions judiciaires

DÉLIBÉRATION CNIL

■ Délibération n° 2005-188 du 8 septembre 2005 portant avis sur le projet de décret en Conseil d'Etat pris pour l'application de l'article 26 (II) de la loi du 6 janvier 1978 modifiée et portant création du système d'information judiciaire JUDEX

R.D.T.I.C
LA REVUE DU DROIT DES TECHNIQUES DE L'INFORMATION ET DE LA COMMUNICATION-
N°58 – NOVEMBRE 2006

PROPRIÉTÉS INTELLECTUELLES, DROIT D'AUTEUR

QUAND DROIT D'AUTEUR RIME AVEC OFFRES SANS SCRUPULES…

Par Melle Astrid Stumpf, Juriste

Un petit clin d'œil au droit d'auteur sur fond de mélodie cubaine…

La High Court of Justice de Londres, juridiction qui tend à se prononcer sur des affaires exceptionnellement complexes, vient de s'exprimer en ce jour sur un litige ayant pour objet les chansons du fameux disque et du non moins connu film « Buena Vista Social Club » interprétées par Omara Portuondo et Eliades Ochoa, et les regrettés Compay Segundo, Ibrahim Ferrer et Ruben Gonzalez.

L'origine du litige remonte déjà à une dizaine d'années. Ces musiciens de renoms avaient alors agi en qualité d'interprètes, enregistrant ainsi quelques fameuses chansons locales, composées des années auparavant. Ces dernières avaient par la suite fait l'objet d'un documentaire réalisé par Wim Wenders, promouvant ainsi la musique cubaine et plus particulièrement ces œuvres à l'échelle mondiale.

La compagnie américaine Peer International Corporation avait alors affirmé détenir la plupart de ces droits depuis les années 1930, accusant la compagnie cubaine Editora Musical de Cuba de s'en être emparés de manière illégale agissant alors pour le compte du gouvernement cubain.

Le gouvernement cubain était ainsi accusé par le biais et ce, selon les dires de Monsieur le juge John Edmund Frederic Lindsay, son « émanation » Editoria Musical de Cuba, de n'avoir respecté l'obligation de droit patrimonial qui découle du droit d'auteur, à savoir notamment l'obligation de contrepartie ou autrement dit de rémunération.

En effet, suite à la révolution cubaine de 1959, les autorités américaines avaient mis en place un embargo empêchant ainsi la poursuite des paiements destinés aux compositeurs alors restés sur le territoire cubain.

Peer International Corporation avait alors poursuivi l'éditeur germano-britannique Termidor Music Publishers qui réclamait pour le compte d'Editoria Musical de Cuba la propriété exclusive de ces droits d'auteur. Le procès avait eu lieu le 11 mai 2005, interrompu suite à un problème technique ne permettant pas de recueillir les témoignages de personnes résidant à Cuba, et s'étant suivi d'une visite de Monsieur de juge Lindsay en territoire castriste.

Ce même juge a aujourd'hui débouté la compagnie Peer International Corporation. En effet, outre le fait que preuve ne pouvait être rapportée avec certitude que les droits d'auteur originaux n'avaient été légalement obtenus, les contrats d'édition des compositions initiales, « offres sans scrupules », ne pouvaient avoir à ce jour de quelconque valeur.

DROIT-TIC .com

R.D.T.I.C

LA REVUE DU DROIT DES TECHNIQUES DE L'INFORMATION ET DE LA COMMUNICATION-
N°58 – NOVEMBRE 2006

NOMS DE DOMAINE ET LIENS HYPERTEXTES, PROPRIÉTÉS INDUSTRIELLES ET COMMERCIALES

RAISON SOCIALE, MARQUE ET NOM DE DOMAINE

Par Mme Marie Roulleaux-Dugage, Chef du service de l'Opposition à l'INPI

Avant première de la conférence 'Trilogie de l'identité de l'entreprise', organisée par INDOM, en partenariat avec l'INPI et la CCIP, le 14 septembre prochain, Marie Roulleaux-Dugage, chef du service de l'Opposition à l'INPI détaille les différents noms que peut utiliser une entreprise.

L'identité commerciale de l'entreprise peut revêtir différentes formes et porter selon les choix stratégiques de l'entreprise sur un ou plusieurs noms. Une société peut se faire connaître sous sa dénomination sociale, état civil équivalent du nom patronymique pour une personne physique, mentionnée pour cela dans les statuts de la société et enregistrée au Registre du Commerce et des Sociétés.

Mais pour communiquer et rallier sa clientèle, une entreprise peut aussi s'identifier sous un nom commercial différent, plus attirant ou plus distinctif. Egalement, elle donne rendez-vous aux internautes sur un site web accessible par son nom de domaine. Et pour finir, si elle veut distinguer les produits qu'elle fabrique ou les services qu'elle rend de ceux de ses concurrents, elle peut déposer une marque.

La marque décodée

La marque est un titre délivré par l'Institut National de la Propriété Industrielle conférant à son titulaire un droit exclusif sur un signe destiné à désigner des produits ou des services précisément énumérés. Ce signe (mot, lettres, chiffres, dessins, couleurs, forme d'un produit, élément sonore … ou la combinaison de ces éléments) doit impérativement être distinctif au regard des produits et des services concernés, c'est à dire qu'il ne doit pas être nécessaire, usuel, ou descriptif de ces produits ou services (la marque GUITARE ne peut être adoptée pour désigner des instruments de musique, de même que la marque BIEN CHAUD pour désigner des vêtements).

Ce signe ne doit pas être trompeur sur une de leur qualité (MEDICA sera rejetée pour désigner des produits diététiques qui ne sont pas à usage médical), ni illicite c'est à dire contraire à l'ordre public et aux bonnes mœurs ou légalement interdit (comme par exemple, pour le dépôt du drapeau d'un pays).

Le choix et les précautions à prendre

Bien souvent se pose la question du choix d'un nom unique ou de l'emploi d'un nom commercial distinct de la dénomination sociale ou de la marque : certaines entreprises n'optent-elles pas pour un seul nom utilisé à titre de dénomination sociale, nom commercial, nom de domaine et marque (à l'instar de CARTIER, DECATHLON, BIC, KILOUTOU...) alors que d'autres possèdent des noms distincts ? La réponse est au carrefour de considérations marketing, juridiques et financières.

S'il est évidemment moins coûteux de communiquer sur un nom unique, cela peut se révéler une formule dangereuse. En cas de conflit avec un droit antérieur, l'usage de ce nom unique pourrait être interdit, ce qui impliquerait de changer de dénomination sociale, de marque, de nom de domaine et de remplacer tous les documents commerciaux ! Il est donc impératif de vérifier la disponibilité du nom choisi et de mesurer les risques de conflit …

En revanche, si l'identité de l'entreprise s'effectue au travers de plusieurs noms, l'action d'un droit antérieur à l'égard de l'un d'entre eux n'affectera pas les autres, ce qui est un avantage non négligeable.

Avant d'adopter un nom, deux précautions sont ainsi à prendre. Tout d'abord, il faut rechercher un terme distinctif sous peine de ne pouvoir empêcher les concurrents de le copier (bois-exotique. com pour désigner une activité de négoce de bois exotiques ne peut être opposé aux tiers opérant dans le même domaine).

Ensuite, il faut vérifier que ce nom ne porte pas atteinte à d'autres droits antérieurs : des recherches d'antériorités doivent être menées au Registre du Commerce et des Sociétés, parmi les marques en vigueur et les noms de domaines. Si la voie est libre, un droit sur ce nom sera constitué dans les plus brefs délais, en réservant son

nom de domaine auprès d'un organisme habilité, en déposant une marque auprès de l'INPI, et en immatriculant sa société. Il faut ainsi éviter qu'un concurrent ne vous devance parce qu'il aura eu connaissance de votre projet ou parce que le nom choisi est dans l'air du temps !

Il est utile à ce stade de faire appel à un professionnel de la propriété industrielle sachant apprécier la disponibilité du nom, mesurer les risques potentiels de conflit et les chances d'en sortir avec succès. Avec plus de 60 000 marques déposées chaque année en France, le nom "libre de tout droit" se fait malheureusement très rare ! Une marque doit donc être déposée seulement si elle possède un degré acceptable de disponibilité et si elle est suffisamment distinctive pour être opposable à un contrefacteur.

Les litiges

En cas de litiges, les actions diffèrent. Une dénomination sociale, un nom commercial ou un nom de domaine seront protégés contre un droit postérieur par l'action judiciaire en concurrence déloyale, qui nécessite de démontrer l'existence d'une faute ayant entraîné un préjudice.

La défense d'une marque est plus simple : il suffit de faire constater la reproduction de la marque antérieure et l'identité des produits et services en cause ou de démontrer l'existence d'un risque de confusion entre les signes et les produits et services concernés. Pour cette raison, le dépôt d'une marque adossé à la réservation d'un nom de domaine reste judicieux !

Deux autres voies extrajudiciaires sont également ouvertes : la procédure d'opposition à l'enregistrement de marque devant l'INPI, ouverte à tout titulaire de marque antérieure et qui est rapide (six mois) ; l'autre voie consiste à recourir à l'arbitrage en saisissant les institutions de règlement agréés par l'ICANN. Le Centre d'Arbitrage et de Médiation de l'OMPI (Cam-OMPI) est aujourd'hui très sollicité pour résoudre de litiges en matière de noms de domaine.

INDOM

R.D.T.I.C
LA REVUE DU DROIT DES TECHNIQUES DE L'INFORMATION ET DE LA COMMUNICATION-
N°58 – NOVEMBRE 2006

DROIT PÉNAL, CRIMINALITÉ INFORMATIQUE, RESPONSABILITÉ

LA SÉCURITÉ DES SITES INTERNET ET DES SYSTÈMES D'INFORMATIONS : QUELLES RESPONSABILITÉS ?

Par M. Nicolas Samarcq, Juriste TIC

L'ouverture des entreprises au réseau internet s'est accompagnée de nouveaux risques juridiques, aggravés par un durcissement législatif en terme de responsabilité.

L'ouverture des entreprises au réseau internet s'est accompagnée de nouveaux risques juridiques, aggravés par un durcissement législatif en terme de responsabilité.

En effet, les défaillances de sécurité, qui rendaient hier l'entreprise victime en cas d'intrusion ou d'entrave à son traitement automatisé de données[1], peuvent désormais la rendre responsable, voire coupable. Ce peut être le cas, par exemple, lorsqu'une faille de sécurité permet l'accès aux données de l'entreprise ou lorsqu'un virus est rediffusé à travers elle.

Les sanctions pénales en cas d'atteinte au traitement automatisé de données

Le fait d'accéder ou de se maintenir frauduleusement dans un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 300 00 euros d'amende[2]. Lorsqu'il en résulte une suppression ou modification des données contenues dans le système, ou une altération de son fonctionnement, la peine est de trois ans d'emprisonnement et de 45000 euros d'amende[3].

De plus, le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données, d'y introduire frauduleusement des données, de supprimer ou modifier frauduleusement les données qu'il contient est puni de cinq ans d'emprisonnement et de 75000 euros d'amende[4].

Enfin, les personnes physiques coupables de ces délits encourent des peines complémentaires dont notamment l'interdiction, pour une durée de cinq ans au plus, d'exercer l'activité professionnelle ou sociale à l'occasion de laquelle l'infraction a été commise[5].

Toutefois, force est de constater que le durcissement pénal des atteintes aux systèmes des données n'est pas appliqué, en raison du faible nombre de victimes qui portent plainte. Et lorsque c'est le cas, les peines prononcées demeurent modestes.

Ainsi, le gérant d'un portail commercial, spécialisé dans le divertissement à caractère pornographique, a porté plainte à la suite d'un courrier électronique lui demandant de fermer son site internet ou d'accepter son rachat pour 3000 € par mois sous menace d'attaques Dos (Déni de service, Denial of service).

Dix jours après l'envoi de cette missive électronique, le site faisait l'objet de plusieurs attaques de type déni de service, destiné à altérer son fonctionnement par une saturation de requêtes. Ces attaques ont fini par entraîner la paralysie totale des services en ligne.

Par jugement du 19 mai 2006, le Tribunal de Grande Instance de Paris a condamné les prévenus à 5 000 euros d'amende pour entrave au fonctionnement d'un système de traitement automatisé de données et à indemniser la société victime de la fraude informatique pour la mobilisation des ressources humaines (9 600 euros) et l'atteinte à l'image (3 000 euros)[6].

L'étendue de la responsabilité du dirigeant et du responsable des traitements

En cas de défaillance de son système d'information, le dirigeant, en tant que chef d'entreprise ou responsable des traitements, risque d'engager sa responsabilité civile et pénale, s'il n'a pas pris les « *mesures techniques et d'organisation appropriées* »[7] pour protéger son système d'information contre des risques internes[8] ou externes.

La Cour de cassation a ainsi jugé qu'une erreur du système informatique de la Caisse d'allocations familiales ne pouvait servir de base légale à une demande de restitution d'allocations indûment perçue, et au contraire a condamné celle-ci à verser des dommages-intérêts d'un montant égal à l'indu réclamé[9]. De manière générale, en cas d'information incorrecte résultante d'un système d'information, qui peut avoir des effets négatifs sur les tiers, le responsable des traitements devra réparer le préjudice subi en versant des dommages et intérêts[10].

Récemment, le Crédit Lyonnais a été condamné à 45 000 € d'amende par la Commission Nationale Informatique et Libertés pour enregistrement abusif de plusieurs de ses clients dans le fichier des incidents de paiement de la Banque de France[11]

Il convient donc d'appréhender de manière précise le standard que les juges exigent du « *bon professionnel* »[12] à travers l'obligation de sécurité de la loi Informatique et Libertés. En effet, la faute, l'imprudence ou la négligence peuvent engager la responsabilité pénale du chef d'entreprise en cas de divulgation de données à caractère personnel[13].

Le dirigeant doit en conséquent prendre les « *précautions utiles* »[14] exigées par la loi Informatique et Libertés pour assurer, « *compte tenu de l'état de l'art et des coûts liés à leur mise en oeuvre, un niveau de sécurité approprié au regard des risques présentés par les traitements et de la nature des données à protéger* »[15].

Les exigences légales de sécurité, obligation de moyens renforcée, seront donc plus strictes dans des domaines sensibles comme les établissements bancaires et la santé.

En conclusion, bien que toutes les entreprises et les systèmes d'information soient différents, toute politique de sécurité informatique doit garantir la disponibilité des ressources et des informations, l'intégrité des données, la confidentialité des données et la traçabilité des accès aux informations[16]. Sur cette base, le « *bon professionnel* »[17] doit bâtir sa politique de sécurité sur des éléments organisationnels et fonctionnels en nommant une personne et son suppléant en charge de la responsabilité de la sécurité du système d'information (le RSSI[18]), en formant son personnel et en rédigeant un code de bonne conduite. A défaut son assurance risque de ne pas couvrir les conséquences pécuniaires de sa responsabilité.

---

1 Les sanctions pénales de la loi n° 88-19 du 5 janvier 1988 sur la fraude informatique (loi GODFRAIN) ont été alourdies.

2 Article L. 323-1 du Code pénal.

3 Ibid.

4 Articles L. 323-2 et L. 323-3 du Code pénal.

5 Article L. 323-5 du Code pénal.

6 Tribunal de grande instance, *Ministère public / Clément P., Elypsal, Thomas P.*, 19 mai 2006, disponible à l'adresse www.legalis.net.

7 Article 17-1 de la directive du 24 octobre 1995.

8 Selon une étude réalisée en 2004 par la société Ibas : en Grande-Bretagne, 69,6% des professionnels ont commis lors de leur départ un vol de propriété intellectuelle auprès de l'entreprise qui les employait, http://www.ibas.fr/nouveautes/articles/UK-2004-05-04/view?searchterm=69.6.

9 Cour de Cassation, 2ème ch. civ., 13 mai 2003, n° de pourvoi 01-21423, http://www.legifrance.gouv.fr/WAspad/Visu?cid=226434&indice=2&table=INCA&ligneDeb=1.

10 Cour d'appel de Bordeaux, 2ème ch., 10 mars 1993, Juris-Data n° 41323. Obs. Lamy droit de l'informatique et des réseaux, éd. 2004, n° 668.

11 Délibération CNIL n° 2006-174 du 28 juin 2006.

12 Cour de Cassation, ch. soc., 31 mars 2003, n° de pourvoi : 01-21490, http://www.legifrance.gouv.fr/WAspad/Visu?cid=219640&indice=3&table=INCA&ligneDeb=1.

13 Article 226-17 du Code Pénal : « *Le fait de procéder ou de faire procéder à un traitement de données à caractère personnel sans mettre en oeuvre les mesures prescrites à l'article 34 de la loi nº 78-17 du 6 janvier 1978 précitée est puni de cinq ans d'emprisonnement et de 300 000 Euros d'amende* ». Article 226-22 § 2 du Code Pénal : « *La divulgation (…) est punie de trois ans d'emprisonnement et de 100 000 € d'amende lorsqu'elle a été commise par imprudence ou négligence* ». Dans un tel cas, l'élément intentionnel de l'infraction est présumé, dès lors qu'il y a eu imprudence ou négligence au regard d'une obligation prévue par la loi.

14 Article 34 de la loi Informatique et Libertés.

15 Article 17-1 de la directive du 24 octobre 1995.

16 Rapport du CLUSIF, *Maîtrise et protection de l'information*, juin 2006, https://www.clusif.asso.fr/fr/production/ouvrages/pdf/Maitrise_et_Protection_de_l_Information.pdf.

17 HENAL (Y.), *Sécurité : Les cinq point faibles les plus fréquents, 6 janvier 2006*, http://www.lemondeinformatique.fr/partnerzone/CA/content_9.

18 Le cas échéant, le RSSI peut être une personne externe à l'entreprise.

R.D.T.I.C
LA REVUE DU DROIT DES TECHNIQUES DE L'INFORMATION ET DE LA COMMUNICATION-
N°58 – NOVEMBRE 2006

INFORMATIQUE ET LIBERTÉS, DROIT SOCIAL, DROIT DU TRAVAIL

LIMITES DE LA SPHÈRE DE VIE PRIVÉE ÉLECTRONIQUE DES SALARIÉS

Par M. Raphaël Rault, Juriste TIC - BRM Avocats

La sphère de « vie privée électronique » des salariés sur leur lieu de travail a été fixée par la jurisprudence de la Cour de cassation.

Par son arrêt « Nikon » du 2 octobre 2001, la chambre sociale de la Cour de cassation avait jugé que « le salarié a droit, même au temps et au lieu de travail, au respect de l'intimité de sa vie privée ».En l'espèce, étaient visés des messages personnels émis par le salarié et reçus par lui grâce à un outil informatique mis à sa disposition pour son travail.

Un arrêt de la Cour de cassation du 17 mai 2005 est venu rappeler que l'employeur ne peut « investiguer » dans les tiroirs du bureau d'un salarié puis accéder à ses fichiers et dossiers informatiques, en l'absence de celui-ci, sans qu'il y ait un risque ou évènement particulier.

Après avoir rendu plusieurs décisions favorables aux salariés quant à l'accès par l'employeur aux dossiers et fichiers stockés par leurs salariés sur le lieu de travail, que ce soit sur le poste informatique ou dans le bureau, la Cour de cassation est venue rappeler les limites des prérogatives accordées aux salariés.

Par un arrêt du 18 octobre 2006, la Cour de cassation fait désormais bénéficier les employeurs d'une présomption simple en affirmant que : « les dossiers et fichiers créés par un salarié grâce à l'outil informatique mis à sa disposition par son employeur pour l'exécution de son travail sont présumés, sauf si le salarié les identifie comme étant personnels, avoir un caractère professionnel de sorte que l'employeur peut y avoir accès hors sa présence ».

En l'espèce, le salarié avait employé un moyen de cryptologie pour empêcher l'accès à ses données informatiques à toute autre personne, y compris son employeur. Ce moyen a été jugé abusif par la Cour de cassation.

L'outil informatique étant mis à la disposition du salarié par son employeur pour les besoins de son activité professionnelle, il paraît légitime pour l'employeur de pouvoir accéder aux données informatiques professionnelles. Il paraît également légitime de lui interdire l'accès aux fichiers et dossiers intitulés « personnel », sphère de vie privée du salarié.

R.D.T.I.C
LA REVUE DU DROIT DES TECHNIQUES DE L'INFORMATION ET DE LA COMMUNICATION-
N°58 – NOVEMBRE 2006

ECONOMIE NUMÉRIQUE, DROIT DES CONTRATS

LA (RE)NÉGOCIATION DES CONTRATS DE COMMUNICATIONS ÉLECTRONIQUES

Par Me. Anne-Katel Martineau, Avocat - SCP COURTOIS LEBEL et Me. Arnaud Tessalonikos Avocat Counsel - SCP COURTOIS LEBEL

Un marché en apparence concurrentiel laisse supposer que les consommateurs, particuliers ou professionnels, peuvent changer facilement d'opérateur et/ou de fournisseur. Or, malgré quelques améliorations, les obst...

Un marché en apparence concurrentiel laisse supposer que les consommateurs, particuliers ou professionnels, peuvent changer facilement d'opérateur et/ou de fournisseur. Or, malgré quelques améliorations, les obstacles à ce changement restent nombreux et variés. Alors, comment envisager concrètement la (re)négociation d'un contrat de communications électroniques afin de conclure un contrat plus avantageux? Est-elle possible de négocier ou même de re-négocier son ou ses contrat(s) de communications électroniques ?

La négociation de ces contrats semble a priori impossible dans la mesure où ils sont pré-rédigés, les consommateurs choisissent donc d'y adhérer ou pas. A fortiori, en l'absence de négociation ab initio il peut paraître curieux d'évoquer leur re-négociation. En pratique, il conviendrait d'envisager une re-négociation lorsqu'il y a eu une négociation préalable. Lorsque celle-ci n'a pas eu lieu, le contrat ne sera pas re-négocié mais pourrait être modifié ou à défaut résilié.

Concrètement, la modification du contrat de communications électroniques est plus facilement envisageable lorsque le client dispose d'un poids économique important constituant un levier. Ce dernier pourra être utilisé dans la re-négociation des contrats de communications électroniques. Nous verrons qu'il existe d'autres leviers qui peuvent être utilisés par les consommateurs.

L'Atelier consacré à ce thème organisé dans le cadre du salon de l'Avocat les 7 et 8 décembre 2006 nous donnera notamment une occasion d'analyser les clauses des contrats de communications électroniques afin de les négocier en connaissance de cause et de les re-négocier si nécessaire. L'objet de cet article consiste, tout d'abord, à exposer les conditions de la (re)négociation des contrats de communications électroniques (Titre I), puis, à donner des éléments permettant de la mettre en oeuvre (Titre II).

Me Anne-Katel MARTINEAU, Avocat, département des Technologies de l'Information et des Communications Electroniques SCP Courtois Lebel.

Me Arnaud Tessalonikos, Avocat counsel, département des Technologies de l'Information et des Communications Electroniques SCP Courtois Lebel

La version complète de cet article sera publiée dans la revue « Les petites affiches » au cours de la seconde quinzaine du mois de novembre 2006. Avec l'aimable autorisation des auteurs et de l'éditeur, la version complète est, dès à présent, disponible sur Droit-Tic :
A-K Martineau et A. Tessalonikos, La (re)négociation des contrats de communication électroniques, Droit-Tic, 02.11.2006, pdf, 8 pages.

http://www.droit-ntic.com/trav/info.php?id_trav=100

DROIT-TIC .com

R.D.T.I.C

LA REVUE DU DROIT DES TECHNIQUES DE L'INFORMATION ET DE LA COMMUNICATION- N°58 – NOVEMBRE 2006

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

QUAND REPRODUCTION À L'IDENTIQUE NE RIME PAS AVEC CONTREFAçON

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

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.

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)

R.D.T.I.C
LA REVUE DU DROIT DES TECHNIQUES DE L'INFORMATION ET DE LA COMMUNICATION-
N°58 – NOVEMBRE 2006

DÉCISION

CA de Paris, 14ème chambre, section B, 26 novembre 2006, SA TISCALI, AFA, FRANCE TELECOM ET ALII / UEJF, J'ACCUSE, SOS RACISME ET ALII

Thèmes
Contenus et comportements illicites, responsabilité

Abstract
Contenus illicites, fournisseur d'accès, obligation de filtrage (oui)
Résumé
Les fournisseurs d'accès doivent, sur le fondemetn de la LCEN, interdire l'accès aux contenus manifestement illicites dont ils ont connaissance

Décision

(Extraits)

Considérant qu'il résulte des écritures des parties et des pièces versées aux débats que le site de l'Association des anciens amateurs de récits de guerre et d'holocauste (Aaargh) diffuse sur le réseau internet, aux adresses "www.aaaegh-international.org" et www.vho.org/aaargh, une compilation d'écrits et de propos antisémites et révisionnistes qui peuvent être téléchargés ;

Qu'il n'est pas contesté que ce site, dont le contenu est constitutif d'infractions pénales, est manifestement illicite et, en propageant des idées que les associations intimées ont pour objet de combattre, cause à celles-ci un dommage que le juge des référés a, par application de l'article 6-1-8 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, le pouvoir de faire cesser en prescrivant aux fournisseurs d'hébergement ou, à défaut, aux fournisseurs d'accès, toutes mesures propres à prévenir ou à mettre fin à ce dommage ;

Considérant que, par ordonnance du 20 avril 2005 rendue au visa de ce texte, le premier juge a, pour l'essentiel :

ordonné, sous astreinte, à la société américaine The Planet.com internet services Inc, seule société à maintenir l'hébergement du site, d'empêcher toute mise à disposition à partir de son serveur et sur le territoire français du site accessible à l'adresse www.vho.org/aaargh,

ordonné, sous astreinte, à chacune des sociétés américaines Olm Llc, Globat Llc et The Planet.com internet services Inc, de fournir tout élément d'identification concernant l'éditeur, le nom du directeur ou du co-directeur de la publication ainsi que les coordonnées complètes de la personne physique ou morale titulaire du contrat d'hébergement,

ordonné la réouverture des débats à l'audience du 30 mai 2005 pour vérifier si les sociétés Olm Llc, Globat Llc et The Planet.com internet services Inc ont exécuté les obligations mises à leur charge et, à défaut, examiner toute demande de liquidation de l'astreinte ainsi que les demandes présentées, le cas échéant, par les associations demanderesses à l'encontre des fournisseurs d'accès afin de voir mettre fin à l'accès en France au site litigieux ;

Considérant que cette décision n'encourt aucun des griefs invoqués par les appelantes, le rejet de la demande de sursis à statuer qu'elles avaient formée étant justifié par la nécessité de prendre immédiatement toutes mesures utiles et la présence des fournisseurs d'accès auxquels l'ordonnance devait être nécessairement rendue commune, s'imposant pour le cas où il devrait être tiré ultérieurement conséquence d'une éventuelle défaillance des sociétés d'hébergement ;

Considérant que par l'ordonnance du 13 juin 2005, le juge des référés, après avoir constaté l'irrégularité affectant les demandes portant sur les liquidations des astreintes formées contre les sociétés Olm Llc, Globat Llc et The Planet.com internet services Inc a, principalement :
- dit n'y voir lieu à liquidation des astreintes, les sociétés prestataires d'hébergement défaillantes n'ayant pas été réassignées pour que soient portées à leur connaissance les demandes formées à ce titre ;
- fait injonction aux sociétés fournisseurs d'accès de mettre en œuvre toutes mesures propres à interrompre l'accès à partir du territoire français au contenu du service de communication en ligne hébergé actuellement à l'adresse www.vho.org/aaargh ;

Considérant que les sociétés appelantes soutiennent, en premier lieu, qu'en prenant une telle décision sans que soient épuisées toutes les possibilités d'atteindre la société Planet.com internet services, seule apte à mettre fin efficacement au dommage "en coupant le mal à la racine", c'est à dire en cessant de stocker les informations illicites, et sans qu'aient été totalement exploités les moyens d'obtenir, auprès des sociétés américaines ayant hébergé ce site, les informations permettant d'identifier les auteurs, le premier juge a méconnu le principe de subsidiarité consacré par l'article 6-1-8 de la loi précitée, lequel ne l'autorisait à prononcer des mesures à l'encontre des fournisseurs d'accès qu'en cas de défaillance des fournisseurs d'hébergement ;

qu'elles reprochent à cet égard aux associations de n'avoir pas exercé tous les recours possibles, notamment par le dépôt d'une plainte avec constitution de partie civile contre l'auteur du site désormais connu, et de s'être abstenues de toute démarche susceptible de conduire à l'exécution effective de l'injonction prononcée par la première ordonnance ;

Considérant que l'article 6-1-2 de la loi du 21 juin 2004 fait peser sur les seuls prestataires d'hébergement une éventuelle responsabilité civile du fait des activités ou des informations stockées qu'ils mettent à la disposition du public en ligne, conformément à la directive européenne n°2000/31 qu'elle transpose ; qu'il s'ensuit que les moyens permettant de mettre en œuvre les mesures destinées à faire cesser le dommage causé par le contenu illicite des informations communiquées doivent être recherchés, en priorité, auprès des sociétés assurant de tels services ;

Considérant que les associations intimées ont assignées devant le juge des référés, le 7 février 2005, les hébergeurs déclarés à cette date, à savoir les sociétés Olm Llc, Globat Llc et The Planet.com internet services Inc pour qu'il leur soit imparti d'empêcher toute mise à disposition du site litigieux, à partir de leur serveur et sur le territoire français et ordonné de fournir tous éléments permettant d'identifier l'éditeur ;
que les fournisseurs d'accès, à l'encontre desquels aucune demande n'était formulée, ont été appelés en cause pour que l'ordonnance leur soit rendue commune dans la perspective énoncée plus haut ; qu'un troisième prestataire d'hébergement, la société Globat Llc, apparue en cours de procédure a été mise en cause ; qu'après l'audience du 14 mars 2005, il est apparu que seule la société Planet.com internet services continuait à héberger le site ; que les associations demanderesses ont réitéré leurs demandes, selon assignations du 29 mars 2005 dirigées contre les sociétés Planet.com internet services et Globat Llc et délivrées à parquet étranger ;
qu'il est établi par les pièces du dossier que les courriers directement adressés à ces sociétés aux Etats-Unis ont été reçus par la société Planet.com internet services et par la société Globat Llc le 28 mars 2005 ; que la première a fait savoir, par courrier électronique du 31 mars, qu'elle n'avait aucun contrôle sur le contenu des sites hébergés et ne serait susceptible de les en retirer que sur injonction de la loi américaine ou sur ordre d'une juridiction compétente des Etats-Unis d'Amérique tandis que la seconde s'est plainte de n'avoir pas reçu une assignation traduite en français ;

Considérant que, bien qu'informées de l'action engagées contre elles, aucune de ces sociétés n'a comparu à l'audience du 18 avril 2005 ; qu'il est démontré par les pièces du dossier que l'ordonnance du 20 avril 2005, signifiée au parquet étranger, a été portée à la connaissance de la société Planet.com internet services le 10 mai 2005 et à celle de la société Olm Llc les 4, 12 et 18 mai 2005 ; qu'aucune de ces sociétés n'a déféré aux injonctions qui leur étaient faites et ne s'est présentée à l'audience de renvoi dont la date était mentionnée sur la décision ;

Qu'il est donc clair que les sociétés de droit américain, ayant assuré ou assurant toujours l'hébergement du site incriminé, n'entendent pas se plier aux injonctions qui leur ont été adressées ni se présenter devant le juge saisi des demandes formées à leur encontre ;

Considérant que c'est précisément pour permettre à l'autorité judiciaire d'intervenir dans les délais les plus rapides afin de faire cesser le dommage occasionné par le contenu d'un service de communication au public en ligne, nonobstant l'inertie des hébergeurs domiciliés à l'étranger ou leur refus d'admettre les mesures de contrainte prononcées contre eux, que le législateur a prévu, à l'article 6-1-8 de la loi précitée, que lesdites mesures peuvent être imposées "à toute personne mentionnée au 2 (les fournisseurs d'hébergement) ou, à défaut, à toute personne mentionnée au 1er (les fournisseurs d'accès) ;

Considérant que les conditions d'application de ce principe de subsidiarité se trouvent remplies en l'espèce dès lors qu'il est démontré que les associations ont accompli les diligences nécessaires pour mettre en cause, par priorité, les sociétés prestataires d'hébergement et que toute possibilité d'agir efficacement à l'encontre de celles-ci s'avère objectivement vaine et en tous cas incompatible avec les exigences d'une procédure conçue pour la prise rapide de mesures dictées par l'intérêt général ;
qu'il ne saurait être fait grief aux associations intimées de n'avoir pas tenté d'obtenir l'exequatur de la décision et la liquidation de l'astreinte vue les difficultés encoures pour aboutir à un résultat positif ; qu'enfin, il ne peut leur être reproché de n'avoir pas déposé plainte avec constitution de partie civile contre l'auteur dont l'identité serait connue alors que la mise en oeuvre des dispositions particulières prévues par la loi du 21 juin 2004 n'est pas soumise à cette condition ;

Que dès lors, le premier moyen soulevé au soutien de l'appel n'est pas fondé ;

Considérant qu'en deuxième lieu, les appelantes font valoir que la mesure ordonnée par le premier juge est inefficace et impropre à faire cesser le dommage, la preuve étant que l'association Aaargh a trouvé les moyens de contourner le blocage d'accès au site vho.org appliqué par les prestataires techniques en exécution de l'ordonnance ; qu'elle est disproportionnée en ce que le blocage opéré entrave non seulement l'accès au site concerné mais également les sites auxquels renverrait le même nom de domaine et constitue une atteinte aux

principe de non-discrimination et de libre concurrence ; qu'elle serait même impossible à mettre en œuvre, la société Suez lyonnaise Telecom soutenant qu'en l'état de sa technologie, elle n'a aucun moyen d'empêcher l'accès à la seule adresse www.vho/aaargh ; qu'elle est contre productive en ce qu'elle permet la diffusion de microsites garantissant l'anonymat de leurs auteurs et n'a pas empêché l'Aaargh de rendre son site accessible à partir de deux nouvelles adresses ; que le filtrage opéré par les fournisseurs d'accès est, en fin de compte, inadapté à la lutte contre les contenus illégaux, la meilleure protection contre leur diffusion passant nécessairement par la poursuite des auteurs des sites ;

Considérant que cette argumentation, déjà développée par les fournisseurs d'accès au moment des débats parlementaires, n'a pas été retenue par le législateur qui, en dépit des difficultés techniques du filtrage, du coût et de la complexité de sa mise en œuvre et de son efficacité contestable, n'a pas exclu le recours à ce procédé et qui, en utilisant la formule "toutes mesures propres à prévenir ou faire cesser un dommage" sans autre précision, a laissé au juge la possibilité d'empêcher ou, pour le moins, de limiter la consultation du contenu mis en ligne dans le cas où, comme en l'espèce, il n'est pas possible d'agir contre les hébergeurs étrangers ;

Qu'une telle mesure, pour imparfaite qu'elle soit, a le mérite de réduire, autant que faire se peut en l'état actuel de la technique, l'accès des internautes à un site illicite et trouve sa place dans la politique menée par l'association des fournisseurs d'accès et de service internet (Afa), selon la Charte Afa du 14 juin 2004, pour lutter contre les contenus odieux tels que ceux faisant l'apologie des crimes contre l'Humanité ou incitant à la haine raciale ;

Que le nomadisme allégué du site de l'Aaargh ne saurait justifier la remise en cause d'une mesure propre à en entraver l'accès ;

Qu'il n'est pas démonté par les prestataires d'accès qui invoquent des difficultés d'ordre technique l'impossibilité pour eux de mettre en place le filtrage effectué par les autres, étant observé que le premier juge a laissé à chacun de ces fournisseurs le soin de mettre en oeuvre tous les moyens dont il peut disposer en l'état de sa structure et de la technologie ;

Considérant enfin, que les principaux fournisseurs d'accès ayant été attraits dans la cause, la discrimination alléguée n'est pas caractérisée et la libre concurrence ne souffre pas de limites disproportionnées ;

Que le deuxième moyen allégué par les appelants est donc inopérant ;

Considérant qu'il est enfin prétendu que la mesure ordonnée, en ce qu'elle n'est pas limitée dans le temps, contredit le caractère provisoire de la décision de référé ; qu'il est demandé à la cour de la cantonner et de la déclarer caduque à l'expiration d'un délai de deux mois à compter du présent arrêt si les associations demanderesses n'ont pas engagé dans ce délai les procédures nécessaires pour rendre exécutoire l'ordonnance du 20 avril 2005 à l'encontre des hébergeurs ou si, dans ce même délai, elles ne se sont pas constituées parties civiles pour la plainte conte X déposée par certaines d'entre elles après du procureur de la République le 25 janvier 2005 ;

Considérant que l'ordonnance rendue en application de l'article 6-1-8 de la loi sur l'économie numérique s'inscrit dans le cadre d'une procédure qui, pour être spécifique, n'en relève pas moins des règles de droit commun ;

Que, cependant, le caractère provisoire de la décision énoncé par l'article 484 du nouveau code de procédure civile ne signifie pas que les mesures ordonnées soient nécessairement limitées dans le temps ; que si une telle limite s'impose lorsque la mesure est prise à titre conservatoire, ainsi qu'il résulte de la jurisprudence versée par les appelantes, elle ne saurait être admise, sauf à vider la décision de son sens et la priver d'efficacité, lorsque l'interruption de l'accès ordonnée par le président a pour but de faire cesser un dommage occasionné par le contenu d'un service de communication en ligne ;

Qu'un tel moyen n'est pas pertinent et les prétentions des appelantes à cet égard ne sauraient être admises ;

Qu'il y a lieu, en conséquence, de confirmer les ordonnances entreprises et de faire application de l'article 700 du ncpc ainsi qu'il sera dit au dispositif ;

. Ordonne la disjonction et la radiation de l'instance concernant Gérard P. ;

. Confirme les ordonnances des 20 avril 2005 et 13 juin 2005 en toutes leurs dispositions ;

. Condamne la société Telecom Italia, la SNC Aol France, la société Suez Lyonnaise Telecom, la société France Telecom Services de communication résidentiels, la société Tele 2 France, la société Neuf Telecom, la société T Online France, la société NC Numericable, l'association des Fournisseurs d'accès et de service internet à payer chacune la somme de 1200 € en application de l'article 700 du ncpc respectivement à L'union des étudiants juifs de France, Sos Racisme Association J'accuse !,

J'accuse ! ....Action internationale pour la justice (Aipj), la Ligue française pour la défense des droits de l'homme et du citoyen, le Mouvement contre le racisme et pour l'amitié entre les peuples (Mrap), le Consistoire central, Union des communautés juives de France, Mémoire 2000, Amicale Union des déportés d'Auschwitz,

. Condamne la société Telecom Italia, la SNC Aol France, la société Suez Lyonnaise Telecom, la société France Telecom Services de communication résidentiels, la société Tele 2 France, la société Neuf Telecom, la société T Online France, la société NC Numericable, l'association des Fournisseurs d'accès et de service internet aux dépens.

Référence : CA de Paris, 14ème chambre, section B, 26 novembre 2006, *SA TISCALI, AFA, FRANCE TELECOM ET ALII / UEJF, J'ACCUSE, SOS RACISME ET ALII*, DROIT-TIC
http://www.droit-tic.com/juris/aff.php?id_juris=84

© J. Le Clainche

R.D.T.I.C
LA REVUE DU DROIT DES TECHNIQUES DE L'INFORMATION ET DE LA COMMUNICATION-
N°58 – NOVEMBRE 2006

C. Cass., Ch. soc., 18 octobre 2006, J. LE F**** / SARL TECHNI-SOFT

Thèmes
droit social, droit du travail, Informatique et libertés

Abstract
Chiffrement des fichiers informatiques par le salarié, faute grave

Résumé
Les dossiers et fichiers créés par un salarié pour l'exécution de son travail sont présumés, sauf si le salarié les identifie comme étant personnels, avoir un caractère professionnel. l'employeur doit donc pouvoir y accéder hors de la présence du salari

Décision

LA COUR DE CASSATION, CHAMBRE SOCIALE, a rendu l'arrêt suivant :

Attendu que M. J. Le F**** a été engagé le 2 octobre 2000 par la société Techni-Soft en qualité d'attaché technico-commercial, par contrat à durée déterminée de six mois qui s'est poursuivi en un contrat à durée indéterminée ; que le 28 février 2002, il a été licencié pour faute grave ayant notamment consisté à empêcher l'accès à ses dossiers commerciaux sur son poste informatique de travail ; que contestant son licenciement et revendiquant le statut de VRP, il a saisi la juridiction prud'homale le 12 avril 2002 ;

Sur le premier moyen :
Attendu que le salarié fait grief à l'arrêt attaqué (Rennes, 21 octobre 2004) d'avoir dit son licenciement fondé sur une faute grave, en violation de l'article L. 122-14-3 du code du travail ;
Mais attendu que les dossiers et fichiers créés par un salarié grâce à l'outil informatique mis à sa disposition par son employeur pour l'exécution de son travail sont présumés, sauf si le salarié les identifie comme étant personnels, avoir un caractère professionnel de sorte que l'employeur peut y avoir accès hors sa présence ; que la cour d'appel, qui a constaté que M. J. Le F**** avait procédé volontairement au cryptage de son poste informatique, sans autorisation de la société faisant ainsi obstacle à la consultation, a pu décider, sans encourir les griefs du moyen, que le comportement du salarié, qui avait déjà fait l'objet d'une mise en garde au sujet des manipulations sur son ordinateur, rendait impossible le maintien des relations contractuelles pendant la durée du préavis et constituait une faute grave ; que le moyen n'est pas fondé ;

Sur le second moyen :
Attendu que le salarié fait grief à l'arrêt de ne pas lui avoir reconnu la qualité de VRP, pour les motifs exposés au moyen, tirés d'une violation de l'article L. 751-2 du code du travail ;

Mais attendu que la cour d'appel, se fondant sur les éléments de fait et de preuve versés aux débats qu'elle a souverainement appréciés, en a déduit que le salarié ne travaillait pas sur un secteur géographique déterminé, ne prenait pas des ordres, exerçait en partie des tâches administratives et n'avait pas développé une clientèle personnelle ; qu'elle a exactement décidé qu'il ne remplissait pas l'ensemble des conditions lui permettant de bénéficier du statut de VRP ;

PAR CES MOTIFS :

REJETTE le pourvoi ;
Condamne M. J. Le F**** aux dépens ;
Vu l'article 700 du nouveau code de procédure civile, rejette la demande de M. J. Le F**** ;
Ainsi fait et jugé par la Cour de cassation, chambre sociale, et prononcé par le président en son audience publique du dix-huit octobre deux mille six.

Référence : C. Cass., Ch. soc., 18 octobre 2006, *J. LE F**** / SARL TECHNI-SOFT*, DROIT-TIC
http://www.droit-tic.com/juris/aff.php?id_juris=85

R.D.T.I.C
LA REVUE DU DROIT DES TECHNIQUES DE L'INFORMATION ET DE LA COMMUNICATION-
N°58 – NOVEMBRE 2006

NORMES REGLEMENTAIRES

Décret n° 2006-1405 du 17 novembre 2006 modifiant le décret n° 64-754 du 25 juillet 1964 relatif à l'organisation du ministère de la justice et instituant une délégation aux interceptions judiciaires

J.O n° 268 du 19 nov. 2006 p. 17391, texte n° 5

NOR: JUSG0660043D

Le Premier ministre,

Sur le rapport du garde des sceaux, ministre de la justice,

Vu le code des postes et des communications électroniques, notamment son article L. 34-1 ;

Vu le code de procédure pénale, notamment ses articles 60-1, 60-2, 74-2, 77-1-1, 77-1-2, 80-4, 100 à 100-7, 706-95 à 706-102 et 800 ;

Vu la loi n° 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des communications électroniques, modifiée par la loi n° 2004-669 du 9 juillet 2004, notamment son article 22 ;

Vu la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, modifiée par la loi n° 2004-669 du 9 juillet 2004, notamment son article 6-II ;

Vu le décret n° 64-754 du 25 juillet 1964 modifié relatif à l'organisation du ministère de la justice ;

Vu le décret n° 87-389 du 15 juin 1987 relatif à l'organisation des services d'administration centrale, modifié par le décret n° 2005-124 du 14 février 2005 ;

Vu l'avis du comité technique paritaire de l'administration centrale du ministère de la justice en date du 9 juin 2006 ;

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

Décrète :

Article 1

Le décret du 25 juillet 1964 susvisé est modifié conformément aux articles 2 à 4 du présent décret.

Article 2

Il est ajouté à l'article 1er-1 un 8° ainsi rédigé :

« 8° Il veille à la mise en oeuvre des missions dévolues à la délégation aux interceptions judiciaires. »

Article 3

Il est ajouté après le sixième alinéa de l'article 1er-2 un alinéa ainsi rédigé :

« f) La délégation aux interceptions judiciaires. »

Article 4

Il est ajouté après l'article 7-3 un article 7-4 ainsi rédigé :

« Art. 7-4. - La délégation aux interceptions judiciaires est chargée, dans le cadre d'orientations générales proposées au ministre par le comité d'orientation des interceptions judiciaires, d'animer et de coordonner les actions visant à assurer la bonne exécution et la maîtrise des coûts des opérations suivantes, lorsqu'elles sont ordonnées lors de procédures judiciaires :

« - les interceptions de correspondances émises par voie de communications électroniques ;

« - les transmissions par les opérateurs de communications électroniques des informations relatives aux contrats d'abonnement souscrits ;

« - les opérations permettant la conservation et la transmission des informations techniques relatives aux caractéristiques des communications électroniques ou permettant l'identification des personnes et des connexions à des services de communications électroniques ainsi que la localisation des équipements utilisés.

« A cet effet, elle coordonne la définition des modalités de mise en oeuvre des réquisitions concernant les opérations judiciaires d'interception de correspondance émises par voie de communications électroniques ainsi que la définition des spécifications judiciaires des dispositifs d'interception, et le suivi technologique de ces dispositifs ; elle participe aux travaux de normalisation des informations transmises aux enquêteurs par les

opérateurs de communications électroniques ainsi qu'à la détermination de la rémunération des opérateurs requis.

« Elle assure la préparation et le suivi des travaux du comité d'orientation des interceptions judiciaires, présidé par le secrétaire général et composé en outre :

« a) Du directeur des affaires criminelles et des grâces ;

« b) Du directeur des services judiciaires ;

« c) Du directeur de l'administration générale et de l'équipement ;

« d) Du directeur général de la police nationale ;

« e) Du directeur général de la gendarmerie nationale ;

« f) Du directeur du budget du ministère de l'économie et des finances ;

« g) Du directeur général des douanes et des droits indirects ;

« h) Du directeur général des entreprises ;

« i) Du haut fonctionnaire de défense auprès du ministre chargé de l'industrie ;

« j) Du commissaire aux télécommunications de défense. »

Article 5

Le ministre d'Etat, ministre de l'intérieur et de l'aménagement du territoire, la ministre de la défense, le ministre de l'économie, des finances et de l'industrie, le garde des sceaux, ministre de la justice, le ministre de la fonction publique et le ministre délégué au budget et à la réforme de l'Etat, porte-parole du Gouvernement, 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 17 novembre 2006.

DROIT-TIC .com

R.D.T.I.C

LA REVUE DU DROIT DES TECHNIQUES DE L'INFORMATION ET DE LA COMMUNICATION-
N°58 – NOVEMBRE 2006

DELIBERATION CNIL

Délibération n° 2005-188 du 8 septembre 2005 portant avis sur le projet de décret en Conseil d'Etat pris pour l'application de l'article 26 (II) de la loi du 6 janvier 1978 modifiée et portant création du système d'information judiciaire « JUDEX »

J.O n° 270 du 22 nov. 2006, texte n° 81

NOR: CNIX0609598X

La Commission nationale de l'informatique et des libertés,

Saisie par le ministre de la défense d'un projet de décret en Conseil d'Etat pris pour l'application de l'article 26 (II) de la loi du 6 janvier 1978 modifiée et portant création du système d'information judiciaire « JUDEX » ;

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 n° 95/46/CE du Parlement européen et du Conseil en date 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 le code pénal ;

Vu le code de procédure pénale ;

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, et notamment ses articles 26 et 41 ;

Vu la loi n° 95-73 du 21 janvier 1995 modifiée, et notamment son article 17-1 ;

Vu la loi n° 2003-239 du 18 mars 2003 pour la sécurité intérieure, et notamment ses articles 21, 22 et 24 ;

Vu le décret n° 78-774 du 17 juillet 1978 modifié pris pour l'application des chapitres Ier à IV et VII de la loi du 6 janvier 1978 précitée ;

Vu le décret n° 79-1160 du 28 décembre 1979 fixant les conditions d'application aux traitements automatisés d'informations nominatives intéressant la sûreté de l'Etat, la défense et la sécurité publique de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ;

Vu la délibération n° 2003-01 du 9 janvier 2003 portant avis conforme sur le projet de décret en Conseil d'Etat portant création du système d'information judiciaire « JUDEX » et faisant application à ce traitement du troisième alinéa de l'article 31 de la loi du 6 janvier 1978 ;

Vu le projet de décret transmis par le ministère de la défense ;

Après avoir entendu M. François Giquel, commissaire, en son rapport, et Mme Catherine Pozzo di Borgo, commissaire du Gouvernement adjoint, en ses observations,

Emet l'avis suivant :

Le ministère de la défense, conformément à l'article 21 (V) de la loi n° 2003-239 du 18 mars 2003 pour la sécurité intérieure et à l'article 26 (II) de la loi n° 78-17 du 6 janvier 1978 modifiée, a saisi pour avis la commission du projet de décret prévu par cette disposition et du dossier de formalités préalables relatif au système d'information judiciaire JUDEX.

Le système d'information judiciaire JUDEX comme le système de traitement des infractions constatées (STIC), mis en oeuvre par la police nationale, constituent des traitements de données à caractère personnel dont les principes de fonctionnement sont fixés par la loi du 18 mars 2003 s'agissant en particulier des finalités de ces fichiers, de leurs modalités d'alimentation et de mise à jour, des catégories de personnes susceptibles d'être inscrites dans ces fichiers et des destinataires des informations.

Le décret d'application de l'article 21 de la loi doit notamment déterminer la liste des contraventions enregistrées, la durée de conservation des informations enregistrées, les modalités d'habilitation des personnels ayant accès aux applications ainsi que, le cas échéant, les conditions dans lesquelles les personnes peuvent exercer leur droit d'accès.

En outre, l'article 26 (II) de la loi du 6 janvier 1978 modifiée prévoit que les traitements intéressant la sûreté de l'Etat, la défense ou la sécurité publique et qui portent sur des données sensibles relevant de l'article 8 de la loi doivent être autorisés par décret en Conseil d'Etat pris

après avis motivé et publié de la CNIL.

Dès lors, le décret soumis à la commission constitue également l'acte réglementaire prévu au titre de cet article.

Sur les finalités du système d'information judiciaire JUDEX :

Aux termes de l'article 1er du projet de décret et conformément à l'article 21 de la loi du 18 mars 2003, le système d'information judiciaire JUDEX a pour finalité de « faciliter la constatation des infractions à la loi pénale, le rassemblement des preuves de ces infractions et la recherche de leurs auteurs ».

A cette fin, l'article 2 du projet de décret prévoit que le système JUDEX est alimenté à partir des procédures établies par les unités de la gendarmerie nationale et par les services de la police lorsqu'une unité de gendarmerie est appelée à en assurer la continuation ou la conduite commune, ainsi que par les agents des douanes habilités à exercer des missions de police judiciaire.

La commission observe à cet égard que, si le paragraphe IV de l'article 21 de la loi du 18 mars 2003 autorise les agents des douanes à accéder aux informations figurant dans les fichiers de police judiciaire, aucune disposition ne leur permet d'alimenter ce fichier.

Dès lors, elle estime qu'il y a lieu de modifier la rédaction de cet article de façon à prévoir que les procédures permettant d'alimenter le système JUDEX sont « établies par les unités de la gendarmerie nationale et par les services de la police ou par les agents des douanes habilités à exercer des missions de police judiciaire, lorsqu'une unité de la gendarmerie est appelée à en assurer la continuation ou la conduite commune ».

Sur les modalités de consultation du système JUDEX à des fins d'enquêtes administratives :

Conformément à l'article 17-1 de la loi du 21 janvier 1995 modifié, l'article 6 du projet de décret définit les conditions de consultation du fichier dans le cadre des enquêtes administratives effectuées notamment lors de l'instruction des demandes d'acquisition de la nationalité française et de délivrance et de renouvellement des titres de séjour et des procédures de recrutement, d'autorisation, d'agrément ou d'habilitation, concernant certains emplois, dont les emplois publics participant à l'exercice des missions de souveraineté de l'Etat et les emplois publics ou privés relevant du domaine de la sécurité ou de la défense, d'une part, et pour l'exercice de certaines missions ou interventions de police administrative, d'autre part.

La commission appelle à nouveau l'attention des pouvoirs publics, comme elle l'a déjà fait à plusieurs reprises, sur les risques graves d'exclusion sociale et d'atteinte aux libertés individuelles, ainsi qu'au respect des droits des personnes que comporte cette utilisation administrative des fichiers de police judiciaire qui leur fait jouer de fait aujourd'hui le rôle d'un casier judiciaire parallèle, alors même qu'ils n'ont pas été conçus pour cette finalité et qu'ils ne bénéficient pas, pour leur alimentation, l'effacement et la consultation des données, des garanties rigoureuses prévues par le code de procédure pénale pour le casier judiciaire national.

La commission a pu constater à maintes reprises, lors des contrôles qu'elle assure au titre du droit d'accès indirect, que les atteintes aux droits des personnes sont réelles, des refus d'embauche ou des licenciements étant décidés sur la seule consultation de ces fichiers et sur la base de signalements injustifiés, erronés ou périmés.

Elle observe aussi que le code de procédure pénale, en ses articles 775 et suivants, a prévu l'exclusion de la mention de certaines condamnations sur les extraits de casier judiciaire transmis aux administrations visées aux articles 776 et 776-1, dans le souci de préserver le droit à l'oubli et de faciliter la réinsertion sociale des personnes condamnées.

La commission estime en conséquence que le décret doit apporter des garanties nouvelles aussi proches que possible de celles entourant aujourd'hui les conditions de transmission des informations extraites du casier judiciaire national.

Tout en prenant acte que le projet de décret prévoit que la consultation à des fins administratives ne peut porter ni sur les données relatives aux victimes, ni sur les données concernant des personnes mises en cause ayant fait l'objet d'une mise à jour ordonnée par le procureur de la République, la commission estime toutefois que des dispositions doivent être prévues afin que le résultat de la consultation ne puisse être communiqué à l'autorité compétente qu'après que le responsable du fichier s'est assuré auprès du procureur de la République compétent qu'aucune décision judiciaire n'est intervenue qui appellerait la mise à jour de la fiche de l'intéressé ou encore qu'aucune requalification judiciaire n'est intervenue qui justifierait la rectification des informations figurant sur cette fiche.

Le dernier alinéa de l'article 6 du projet de décret doit en conséquence être complété en ce sens.

Relevant que le législateur n'a admis la consultation administrative des fichiers de police judiciaire que « dans la stricte mesure exigée par la protection de la sécurité des personnes et la défense des intérêts fondamentaux de la nation », la commission estime qu'il convient de s'interroger sur le bien-fondé d'une consultation

systématique à des fins administratives des fichiers de police judiciaire s'agissant des personnes mises en cause pour des faits relevant d'une contravention de 5e classe ou de certains délits, qui ne mettraient pas en cause la sécurité des personnes ou la défense des intérêts fondamentaux de la nation.

Enfin, lorsque le fichier est consulté par des personnels investis de missions de police administrative, comme le prévoit l'article 7 du projet de décret, la commission estime que pour garantir le caractère limité de cette consultation le deuxième alinéa de cet article du projet de décret doit être complété de la façon suivante : « Dans ce cas, l'accès à l'information est limité à la seule connaissance de l'enregistrement de l'identité de la personne concernée dans le traitement en tant que mis en cause ».

La commission rappelle en outre qu'aux termes de l'article 10 de la loi du 6 janvier 1978 modifiée, aucune décision produisant des effets juridiques à l'égard d'une personne ne peut avoir pour seul fondement un traitement automatisé de données à caractère personnel destiné à définir le profil de l'intéressé ou à évaluer certains aspects de sa personnalité.

Sur le champ d'application du fichier :

La commission observe que sont susceptibles d'être inscrites dans le système JUDEX les personnes mises en cause telles que définies à l'article 21 de la loi du 18 mars 2003, et les victimes, et en aucun cas les témoins.

Elle constate ensuite que, conformément à l'article 21 de la loi précitée, les infractions susceptibles de donner lieu à inscription dans le système JUDEX concernent non seulement les crimes et délits, mais également la totalité des contraventions de 5e classe contre les biens (articles R. 635-1 à R. 635-8), contre les personnes (articles R. 625-1 à R. 625-9) et contre la nation, l'Etat ou la paix publique (articles R. 645-1 à R. 645-12).

La commission estime devoir appeler à nouveau l'attention du ministère de la défense et du ministère de la justice sur les risques que comporte une telle centralisation, dans un fichier national, d'informations de police judiciaire, eu égard, d'une part, à l'extrême diversité des infractions visées, tant par leur nature que par leur degré de gravité et, d'autre part, à leur utilisation dans le cadre de multiples enquêtes administratives, et sur la nécessité de prendre des mesures particulières destinées à prévenir tout fichage non contrôlé, erroné ou abusif des personnes et tout usage d'un tel fichier à des fins étrangères à celles pour lesquelles il est constitué.

En ce qui concerne les contraventions de 5e classe, la commission considère à cet égard que, si le législateur a permis d'étendre la liste des contraventions de 5e classe susceptibles de donner lieu à un signalement dans le système JUDEX, il ressort néanmoins des travaux préparatoires que le Gouvernement ne devrait pouvoir faire usage de cette possibilité que lorsque cette extension est rendue nécessaire par la sauvegarde de la sécurité intérieure. Or une telle nécessité n'apparaît pas pouvoir être invoquée pour l'ensemble des contraventions visées au projet de décret.

Dès lors elle considère que la liste des contraventions de 5e classe doit être réexaminée et justifiée.

Sur la mise à jour du fichier :

La commission observe qu'en vertu de la loi le système JUDEX est placé sous le contrôle du procureur de la République territorialement compétent, qui peut décider que les informations figurant dans ces fichiers doivent être effacées, complétées ou rectifiées.

Il relève ainsi du pouvoir d'appréciation du procureur d'ordonner, au vu de la procédure, l'effacement ou la mise à jour des informations notamment en cas de décision de relaxe, d'acquittement, de non-lieu ou encore de classement sans suite pour insuffisance de charge, selon les modalités définies par l'article 21 (III) de la loi du 18 mars 2003.

Pour permettre l'application effective de ces règles, il importe que toute disposition soit prise afin que les procureurs puissent transmettre sans délai au gestionnaire du fichier leurs décisions d'effacement ou de mise à jour.

La mise à jour immédiate, systématique, et rigoureuse des informations enregistrées, mise à la charge des procureurs, constitue en effet une garantie essentielle pour les personnes concernées, ce d'autant plus que les fichiers de police judiciaire sont aussi consultés à des fins d'enquête administrative, dans le cadre en particulier de procédures d'embauche ou d'accès à des emplois de sécurité.

La commission s'étonne à cet égard que le projet de décret ne comporte aucune précision quant aux diligences qui incombent dès lors aux procureurs ; elle estime en conséquence que doivent figurer expressément dans le projet de décret les modalités de transmission des informations nécessaires à la mise à jour et à l'effacement des données.

La commission appelle à nouveau fermement l'attention des ministères concernés sur la nécessité de mettre en place rapidement des liaisons informatiques sécurisées entre les parquets et le ministère de l'intérieur, afin d'assurer un contrôle effectif des parquets sur le fonctionnement des fichiers de police judiciaire et une mise à jour sans délai de ce fichier.

Sur les catégories d'informations traitées et sur les

données sensibles :

Les données à caractère personnel enregistrées dans JUDEX sont, pour les personnes mises en cause, l'identité (nom, nom marital, nom d'emprunt officiel, prénoms, sexe), les surnoms et les alias s'il y a lieu, les date et lieu de naissance, la situation familiale, la filiation, la nationalité, l'adresse, l'état de la personne (modes opératoires et informations relevant de l'article 8 de la loi du 6 janvier 1978 modifiée lorsque ces renseignements sont susceptibles d'éclairer le mode opératoire ou les mobiles de l'infraction, références des affaires judiciaires pour lesquelles la personne est mise en cause, suites judiciaires transmises par le procureur de la République territorialement compétent dans les conditions du projet de décret), la profession, le signalement et la photographie.

Pour les victimes, sont enregistrés : identité (nom, nom marital, nom d'emprunt officiel, prénoms, sexe), date et lieu de naissance, situation familiale, nationalité, adresse, profession, état de la personne (références des affaires judiciaires dans lesquelles la personne est victime, suites judiciaires transmises par le procureur de la République territorialement compétent dans les conditions du projet de décret), signalement et photographie pour les personnes disparues et les corps non identifiés, uniquement.

Sont également enregistrées des informations non nominatives ou indirectement nominatives concernant les faits objets de l'enquête, les lieux, dates et modes opératoires, ainsi que des informations et images relatives aux objets.

La commission considère que la finalité du fichier justifie la collecte et l'enregistrement pour des motifs d'intérêt public de données à caractère personnel relevant de l'article 8 de la loi, à la condition toutefois que cette collecte et cet enregistrement, ainsi que le prévoit l'article 4 du projet de décret, ne soient effectués que dans les seuls cas où ces informations résultent de la nature ou des circonstances de l'infraction ou se rapportent à des signes physiques particuliers, objectifs et permanents, en tant qu'éléments de signalement des personnes et dès lors que ces éléments sont nécessaires à la recherche et à l'identification des auteurs des infractions répertoriées dans le système JUDEX.

Sur la durée de conservation :

Le projet de décret précise que les données concernant les personnes majeures mises en cause seront, en principe, conservées vingt ans à compter de la date d'établissement de la procédure. Toutefois, les informations concernant certains crimes et délits figurant sur une liste annexée au décret seront conservées pendant quarante ans et les informations relatives aux contraventions de 5e classe, aux délits routiers, aux délits d'abandon de famille et de non-représentation d'enfant et aux délits d'usage de stupéfiant seront conservées pendant cinq ans.

S'agissant des mineurs, le projet de décret prévoit que la durée de conservation de principe est de cinq ans, exception faite de certains crimes et délits graves énumérés dans deux listes annexées au décret, qui déterminent des durées de conservation, respectivement, de dix et vingt ans.

La durée de conservation des informations concernant les victimes est au maximum de quinze ans, sous réserve de la faculté qui leur est ouverte de demander la suppression des informations qui les concernent dès lors que l'auteur de l'infraction aura été définitivement condamné. Cette durée est prolongée jusqu'à la découverte des objets lorsque l'infraction porte sur des oeuvres d'art, des bijoux ou des armes.

Si, dans leur principe, de telles durées peuvent être justifiées par la finalité de recherche et d'identification des auteurs d'infractions, la possibilité désormais reconnue par la loi de consulter, dans le cadre d'enquêtes administratives, les informations ainsi conservées rend d'autant plus impératif la mise à jour et l'effacement d'informations enregistrées selon les règles précédemment définies.

Sur les destinataires des informations et les modalités d'habilitation :

Peuvent être destinataires des informations enregistrées dans le système JUDEX, pour les besoins des enquêtes judiciaires et conformément au paragraphe IV de l'article 21 de la loi du 18 mars 2003 :

- les personnels des services de la gendarmerie nationale et de la police nationale, ainsi que les agents des douanes habilités à effectuer des missions de police judiciaire, qui exercent des missions de police judiciaire et ont fait l'objet d'une désignation par l'autorité hiérarchique ;

- les autres personnels de l'Etat investis par la loi d'attributions de police judiciaire ;

- les magistrats du parquet ;

- les magistrats instructeurs, pour les recherches relatives aux infractions dont ils sont saisis ;

- les organismes de coopération internationale en matière de police judiciaire et les services de police étrangers, dans les conditions énoncées à l'article 24 de la loi pour la sécurité intérieure du 18 mars 2003.

En outre, conformément à l'article 17-1 de la loi du 21 janvier 1995, modifié par l'article 25 de la loi du 18 mars

2003, le projet de décret prévoit que les personnels de la gendarmerie et de la police spécialement habilités ainsi que les personnels investis de missions de police administrative désignés selon les mêmes procédures peuvent avoir accès aux fichiers à des fins administratives.

Compte tenu du très grand nombre d'utilisateurs potentiels et de la sensibilité des fichiers concernés ainsi que de la possibilité nouvelle pour les personnels de la police et de la gendarmerie nationale d'accéder « par tous moyens techniques mobiles aux données du fichier », il est impératif que des règles d'habilitation rigoureuses de ces personnels soient définies.

Or, contrairement à ce que prévoit l'article 21 (IV) de la loi du 18 mars 2003, le projet de décret ne précise pas les modalités d'habilitation des personnels accédant aux fichiers dans le cadre de leurs missions de police judiciaire.

La commission estime en conséquence que le projet de décret devrait être complété de façon à préciser que ces personnels doivent être individuellement désignés et spécialement habilités et à indiquer l'autorité qui la délivre, la nature des données auxquelles l'habilitation donne accès, les catégories de personnel ou de fonctions bénéficiant de cette habilitation.

Elle considère qu'il doit en être de même d'une part pour les personnels des services de police et de gendarmerie susceptibles d'avoir accès au fichier à des fins administratives et qui doivent être « spécialement habilités à cet effet » selon la loi et, d'autre part, pour les personnels administratifs qui doivent être « désignés selon les mêmes procédures ».

Par ailleurs, la commission prend acte qu'un système de journalisation des interrogations permet de conserver trace des connexions pendant trois ans et un historique des requêtes effectuées est mis en oeuvre au niveau central.

De même, toute mise à jour (création, modification, suppression) provoquera l'enregistrement pendant trois ans des informations relatives au personnel qui y aura procédé.

Sur l'exercice du droit d'accès :

L'article 8 du projet de décret relatif au système JUDEX prévoit que « le droit d'accès s'exerce d'une manière indirecte, dans les conditions prévues par l'article 41 de la loi du 6 janvier 1978 susvisée, par demande portée devant la Commission nationale de l'informatique et des libertés, pour l'ensemble des données ». Son second alinéa dispose que « la commission peut constater, en accord avec le ministère de la défense, que des données à caractère personnel enregistrées ne mettent pas en cause la sûreté de l'Etat, 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 ».

La commission observe que l'article 22 de la loi du 18 mars 2003 a modifié l'article 39 de la loi du 6 janvier 1978 (devenu, par la loi du 6 août 2004, l'article 41) de façon que « lorsque la commission constate, en accord avec le responsable du traitement, que la communication des données qui y sont contenues ne met pas en cause ses finalités, la sûreté de l'Etat, la défense ou la sécurité publique, ces données peuvent être communiquées au requérant ». En outre, son dernier alinéa dispose que : « lorsque le traitement est susceptible de comprendre des informations dont la communication ne mettrait pas en cause les fins qui lui sont assignées, l'acte réglementaire portant création du fichier peut prévoir que ces informations peuvent être communiquées au requérant par le gestionnaire du fichier directement saisi ».

Dès lors que la loi du 18 mars 2003 ouvre au gestionnaire du fichier concerné une possibilité de communiquer directement aux requérants les informations dont la communication ne mettrait pas en cause la finalité du fichier considéré, la commission estime qu'il y a lieu de prévoir, pour les personnes inscrites dans le système JUDEX en tant que victimes, la communication directe par les soins du ministère de la défense du contenu de leur fiche.

La saisine directe du responsable du traitement, même limitée aux victimes, permettra en outre de réduire la durée des procédures, ce qui va dans le sens d'une meilleure garantie des droits individuels.

Pour tenir compte des dispositions du premier alinéa de l'article 41 de la loi du 6 janvier 1978 modifiée, et dans le même souci de répondre plus rapidement et plus efficacement aux requérants, la commission considère en outre que la rédaction nouvelle de l'article 41 de loi n'impose plus de subordonner l'exercice du droit d'accès indirect au recueil de l'accord du procureur de la République ni à l'exigence que la procédure soit judiciairement close.

En conséquence, l'article 8 du projet de décret relatif à JUDEX devrait être modifié de façon, d'une part, à prévoir l'exercice du droit d'accès direct pour les victimes et, d'autre part, à supprimer les deux conditions supplémentaires prévues par cet article pour permettre la communication, avec l'accord du ministère de la défense, des données les concernant aux personnes mises en cause.

Sur l'information des personnes :

Aucune mesure d'information n'est prévue ni à l'égard des personnes mises en cause, ni à l'égard des victimes.

Le ministère de la défense invoque les dispositions de l'article 32 (VI) de la loi du 6 janvier 1978 modifiée qui prévoit une dérogation à l'obligation générale d'information des personnes s'agissant des traitements de données ayant pour objet la prévention, la recherche, la constatation ou la poursuite d'infractions pénales.

Toutefois, dans la mesure où le législateur a expressément reconnu aux personnes faisant l'objet d'une inscription dans les fichiers de police judiciaire la possibilité, sous certaines conditions, de demander la rectification des données en cas de requalification judiciaire et, s'agissant des victimes, l'effacement des données les concernant, la commission estime que l'information des personnes sur l'existence et les conditions d'exercice de ces droits, ainsi que sur leur droit d'accès, doit être reconnue et garantie par des mesures spécifiques.

La commission considère en conséquence que le décret doit être complété afin que toutes dispositions soient prises pour que les personnes concernées soient clairement et précisément informées de leurs droits et tout particulièrement des conditions d'exercice de leur droit d'accès, de leur droit de demander, le cas échéant, que la qualification judiciaire des faits soit substituée à la qualification initiale telle qu'elle est enregistrée dans le système JUDEX, ainsi que du droit de s'adresser au procureur de la République territorialement compétent pour solliciter la mise à jour des informations les concernant.

Ainsi, il pourrait être envisagé qu'outre des mesures d'information générale, par exemple sur le site internet de la gendarmerie nationale, un affichage dans le local d'accueil du public de chaque unité élémentaire de gendarmerie et une mention sur l'attestation de dépôt de plainte remise aux victimes soient notamment prévus, ainsi que le prévoyait le dossier de formalités préalables relatif à la création du système JUDEX qui a été soumis à la commission au mois de janvier 2003.

Sur les échanges internationaux de données avec les organismes de coopération internationale en matière de police et les services de police étrangers :

Le projet de décret prévoit que les informations du fichier JUDEX peuvent faire l'objet d'une cession aux organismes de coopération internationale en matière de police judiciaire (Interpol, Europol, Schengen) et aux services de police étrangers qui présentent un niveau de protection suffisant, dans le respect des engagements internationaux dont ces données font l'objet ou peuvent faire l'objet, d'autre part, à permettre à ces organismes d'alimenter indirectement le fichier JUDEX.

Ces différents échanges ne peuvent être effectués qu'à la condition, expressément inscrite à l'article 24 de la loi du 18 mars 2003, que les services concernés « présentent, pour la protection des données personnelles, des garanties équivalentes à celles du droit interne, dans le cadre des engagements internationaux régulièrement introduits dans l'ordre juridique interne ». Dès lors ils n'appellent pas d'observations de fond.

La commission estime en conséquence que pour être conforme à ces dispositions il y aurait lieu de reprendre, à l'article 10 du projet de décret, les termes de l'article 24 de la loi.

Le président,

A. Türk