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

ANALYSES

AU J.O AU MOIS D' AVRIL 2007

DÉLIBÉRATIONS CNIL

RDTIC

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

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

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

Conseil scientifique

Informations légales

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

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

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

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

DROIT-TIC .com

R.D.T.I.C

LA REVUE DU DROIT DES TECHNIQUES DE L'INFORMATION ET DE LA COMMUNICATION-
N°63– AVRIL 2007

ANALYSES

AU J.O AU MOIS D' AVRIL 2007

■ Décret n° 2007-510 du 4 avril 2007 relatif à l'Autorité de régulation des mesures techniques instituée par l'article L. 331-17 du code de la propriété intellectuelle

■ Avis de la commission générale de terminologie et de néologie du 20 avril 2007

DÉLIBÉRATIONS CNIL

■ Dél. n° 2007-039 du 20 février 2007 portant refus d'autorisation de la mise en oeuvre par la société Kimberly-Clark SNC d'un traitement automatisé de données à caractère personnel ayant pour finalité la mise en place d'un dispositif d'alerte professionnelle

■ Dél. n° 2007-039 du 20 février 2007 portant refus d'autorisation de la mise en œuvre par la société Crown Worldwild SAS d'un traitement automatisé de données à caractère personnel ayant pour finalité la mise en place d'un dispositif d'alerte professionnelles

■ Dél. n° 2007-021 du 8 février 2007 autorisant à titre expérimental, pendant un an, la mise en œuvre par la société RIA France d'un traitement automatisé des ordres de transfert internationaux de fonds ayant notamment pour finalité la lutte contre le blanchiment de capitaux…

■ Dél. n° 2007-041 du 8 mars 2007 portant autorisation de la mise en œuvre par ADP d'un traitement de données à caractère personnel reposant sur la reconnaissance par empreinte digitales et ayant pour finalité le contrôle de l'accès…

■ Dél. n° 2006-281 du 14 décembre 2006 sanctionnant la société Tyco healthcare France

DROIT-TIC .com

R.D.T.I.C

LA REVUE DU DROIT DES TECHNIQUES DE L'INFORMATION ET DE LA COMMUNICATION-
N°6 3 – AVRIL 2007

INFORMATIQUE ET LIBERTÉS, VIEPRIVÉE

LE SECOND DÉCRET D'APPLICATION DE LA LOI INFORMATIQUE ET LIBERTÉS

Par M. Nicolas Samarcq

Le second décret d'application de la loi précise les modalités d'exercice des obligations d'information incombant aux responsables de traitements, les droits des personnes à l'égard de ces traitements, ainsi que la mise en œuvre d'un référé « mesures utiles » spécifique au secteur public.

Le second décret d'application de la loi[1] précise les modalités d'exercice des obligations d'information incombant aux responsables de traitements, les droits des personnes à l'égard de ces traitements, ainsi que la mise en œuvre d'un référé « mesures utiles » spécifique au secteur public.

 Les modalités d'exercice des obligations d'information[2] relatives aux traitements

A l'égard des personnes concernées :

Les responsables de traitements doivent porter ces informations directement à la connaissance des personnes auprès desquelles sont recueillies des données à caractère personnel sur le support de collecte ou, à défaut, sur un document préalablement porté à leur connaissance en caractères lisibles.

Dans les mêmes conditions, ils les informent également des coordonnées du service compétent auprès duquel ces personnes peuvent exercer leurs droits d'opposition, d'accès et de rectification.

Lorsque la collecte des données est opérée oralement à distance, il est donné lecture de ces informations aux personnes[3] en leur indiquant qu'elles peuvent, sur simple demande, même exprimée oralement, recevoir postérieurement ces informations par écrit.

Ces informations peuvent être communiquées aux personnes[4], avec leur accord, par voie électronique.

Si ces informations relatives aux traitements sont portées à la connaissance des personnes[5] par voie d'affichage, il doit être indiqué qu'elles peuvent, sur simple demande orale ou écrite, recevoir ces informations sur un support écrit.

Enfin, en cas de transfert de données personnelles vers un Etat non membre de l'Union européenne, le responsable du traitement doit informer, dans les mêmes conditions, les personnes[6] sur :

- le ou les pays d'établissement du destinataire des données, et si ce ou ces pays figurent dans la liste de la Commission européenne autorisant ce transfert[7], ou dans le cas contraire, il doit être fait mention de l'exception prévue par loi Informatique et Libertés permettant ce transfert[8] ;

- la nature des données transférées ;

- la finalité du transfert envisagé ;

- les catégories de destinataires des données ;

- le niveau de protection offert par le ou les pays tiers.

Lorsque le transfert est envisagé postérieurement à la collecte des données à caractère personnel, celui-ci ne peut intervenir que dans un délai de quinze jours suivant la réception par l'intéressé des informations mentionnées ci-dessus.

A l'égard des tiers :

Lorsque des données à caractère personnel ont été transmises à un tiers, le responsable du traitement qui a procédé à leur rectification en informe sans délai ce tiers, qui doit procéder également sans délai à leur rectification.

 Les modalités d'exercice des droits des personnes à l'égard des traitements :

L'exercice du droit d'accès direct :

Sauf disposition législative ou réglementaire contraire, une copie des données à caractère personnel qui concernent le demandeur et pendant une durée suffisante peut être obtenue immédiatement par ce dernier.

Lors de la délivrance de la copie demandée, le responsable de traitement atteste, le cas échéant, du paiement de la somme perçue à ce titre.

L'exercice du droit d'opposition :

Pour faciliter l'exercice du droit d'opposition, la personne doit être mise en mesure d'exprimer son choix avant la validation définitive de ses réponses.

Lorsque la collecte des données intervient par voie orale, la personne est mise en mesure d'exercer son droit d'opposition avant la fin de la collecte des données le concernant.

Le responsable du traitement auprès duquel le droit d'opposition a été exercé informe sans délai de cette opposition tout autre responsable de traitement qu'il a rendu destinataire des données à caractère personnel qui font l'objet de l'opposition.

Ces dispositions prohibent donc, par exemple, les formulaires de vente sur internet qui obligent l'internaute à accepter des conditions générales de vente dans lesquelles le droit de s'opposer à la cession de ses données personnelles auprès des partenaires commerciaux du vendeur s'exerce a posteriori et par écrit.

La durée d'exercice du droit de rectification

L'héritier d'une personne décédée qui souhaite la mise à jour des données concernant le défunt doit, lors de sa demande, apporter la preuve de sa qualité d'héritier par la production d'un acte de notoriété ou d'un livret de famille.

Les demandes :

- Les demandes écrites des personnes tendant à la mise en œuvre de leurs droits d'accès, de rectification et d'opposition, sont signées et accompagnées de la photocopie d'un titre d'identité portant leur signature. Elles précisent, en outre, l'adresse à laquelle doit parvenir la réponse.

Lorsqu'il existe un doute sur l'adresse indiquée ou sur l'identité du demandeur, la réponse du responsable du traitement peut être expédiée sous pli recommandé sans avis de réception. La vérification de l'adresse ou de l'identité du demandeur s'effectuera lors de la délivrance du pli.

Réciproquement, lorsque le responsable du traitement ou le correspondant à la protection des données (CIL) n'est pas connu de la personne désirant exercer ses droits, celle-ci peut adresser sa demande au siège de la personne morale ou de l'autorité publique. La demande est alors transmise immédiatement au responsable du traitement.

- Les demandes présentées sur place doivent justifier par tout moyen de l'identité de la personne auprès du responsable du traitement. La personne peut se faire assister d'un conseil de son choix.

- La demande peut être également présentée par un mandataire, après justification de son mandat, de son identité et de l'identité du mandant.

Les réponses :

Les codes, sigles et abréviations figurant dans la réponse délivrée par le responsable de traitement doivent être explicités, si nécessaire sous la forme d'un lexique.

Lorsque la demande ne peut être satisfaite immédiatement, il est délivré à son auteur un avis de réception, daté et signé. Le responsable du traitement dispose alors d'un délai de deux mois, à compter de la réception de la demande, pour répondre à la personne.

Si la demande est imprécise ou ne comporte pas tous les éléments permettant au responsable du traitement de procéder aux opérations qui lui sont demandées, celui-ci invite le demandeur, par lettre remise contre signature ou par voie électronique, à les lui fournir avant l'expiration du délai de 2 mois. Cette demande de compléments d'information suspend ledit délai.

Sauf lorsque la demande est manifestement abusive, les décisions du responsable du traitement de ne pas donner une suite favorable à la demande qui lui est présentée sont motivées et mentionnent les voies et délais de recours ouverts pour les contester.

Le silence gardé pendant plus de deux mois par le responsable du traitement sur une demande vaut décision de refus.

Ce formalisme applique donc aux responsables de traitements du secteur privé les règles classiques du droit administratif.

 Le référé « mesures utiles » spécifique au secteur public

Le juge administratif peut être saisi en référé, sur le fondement de la loi Informatique et Libertés[9], d'une demande relative au prononcé de toutes mesures utiles de nature à éviter toute dissimulation ou toute disparition de données à caractère personnel par l'Etat, une collectivité territoriale, toute autre personne publique ainsi que toute personne privée chargée d'une mission de service public.

A ce titre, le juge des référés peut prononcer des mesures provisoires ou conservatoires, et plus généralement des injonctions sous astreintes, à condition que l'urgence le justifie, qu'elles soient utiles et ne fassent obstacles à l'exécution d'une décision administrative.

Enfin, il est à noter que ce décret d'application comporte un ensemble de dispositions entrant dans le détail de l'organisation, du fonctionnement et des procédures internes de la Commission Nationale Informatique et Libertés (CNIL).

Or, la CNIL a rappelé que la loi Informatique et Libertés lui permet de fixer elle-même les règles relatives à son organisation et son fonctionnement. Dès lors, la CNIL a estimé que les termes de la loi « *auraient pu conduire à limiter plus étroitement l'intervention du pouvoir réglementaire dans des matières que le législateur a expressément renvoyées au règlement intérieur de la CNIL, autorité administrative indépendante* »[10].

Il est donc à regretter que le gouvernement n'ait pas suivi l'ensemble des propositions d'amendement de la CNIL concernant son organisation interne.

Par exemple, après avoir rappelé que les délibérations de la CNIL avaient augmenté de 570 % entre 2003 et 2006, le gouvernement n'a pas suivi la proposition de l'autorité administrative indépendante de diminuer le

délai de transmission au commissaire du Gouvernement des dossiers inscrits à son ordre au jour (six jours avant la date de la séance contre huit jours dans le décret). En effet, « *l'examen d'un dossier, par la commission, voire l'adoption d'une délibération, ne sauraient être subordonnés à la transmission des dossiers au commissaire du Gouvernement qui constitue une règle de stricte procédure* ».

Plus inquiétant, la CNIL n'a pas été suivie sur sa demande de suppression du régime d'avis favorable implicite concernant ses avis obligatoires sur les projet de loi et décrets relatifs à la protection des personnes à l'égard des traitements automatisés[11].

Nicolas Samarcq - Juriste TIC
www.lexagone.com
Membre de l'AFCDP, Association Française des Correspondants aux Données Personnelles

R.D.T.I.C
LA REVUE DU DROIT DES TECHNIQUES DE L'INFORMATION ET DE LA COMMUNICATION-
N°6 3 – AVRIL 2007

PROPRIÉTÉS INTELLECTUELLES, PROPRIÉTÉS INDUSTRIELLES ET COMMERCIALES

LA LÉGITIMATION DES MARQUES DE DÉFENSE ?

M. Fabrice Bircker et M. Bruno Raibaut

Par une série de décisions rendues en l'espace de moins d'une année, la Cour de Cassation est revenue sur sa jurisprudence en matière de déchéance des marques faisant l'objet d'enregistrements parallèles.

Il est fréquent qu'une entreprise détienne plusieurs marques dont les signes respectifs sont extrêmement proches les uns des autres, sans pour autant qu'elles les utilise toutes sur le marché.

De telles marques prennent le nom d'enregistrements parallèles.

Cette situation, où un acteur économique détient des marques pouvant paraître à première vue inutiles, peut avoir diverses origines et être plus ou moins voulue.

Ainsi, le titulaire d'une marque peut-il avoir souhaité moderniser sa marque initiale et procéder au dépôt de la nouvelle variante.

L'exploitant d'une marque peut également avoir voulu consolider ses droits en rachetant une marque analogue à la sienne déposée antérieurement.

Autre cas de figure : plusieurs marques proches les unes des autres peuvent avoir été protégées dans la seule perspective d'être opposées aux tiers qui utiliseraient des marques identiques ou similaires et ce, afin d'accroître le périmètre de protection de la seule marque présente sur le marché (dans cette situation les marques non utilisées sont également dénommées "marques de barrage", l'expression étant pour le moins explicite).

Parallèlement, dans le souci de désengorger le Registre National des Marques, l'article L. 714-5 du Code de la Propriété Intellectuelle (CPI) permet à toute personne intéressée de solliciter en justice la déchéance d'une marque, lorsque celle-ci n'est plus exploitée depuis plus de cinq années consécutives.

Cette disposition trouve sa justification dans le fait que la marque est, par essence, un signe distinctif et qu'elle a donc vocation à être exploitée.

En d'autres termes, une marque trop longtemps absente du marché perd sa raison d'être et quiconque en éprouve l'intérêt doit pouvoir la faire disparaître.

On le perçoit rapidement, l'article L. 714-5 CPI ne fait pas bon ménage avec les enregistrements parallèles de marques.

Et, lorsque le titulaire d'enregistrements parallèles de marques est attaqué en déchéance de ses droits, se pose la question de savoir dans quelle mesure cette personne peut se prévaloir de l'exploitation de l'une de ses marques, afin de faire échapper les autres à la déchéance, lesquelles sont, par hypothèse, non utilisées et extrêmement proches de la seule marque utilisées.

A première vue, la réponse se trouverait dans le texte même de l'article L. 714-5 CPI.

En effet, le deuxième alinéa de ce texte dispose que "*l'usage de la marque sous une forme modifiée n'en altérant pas le caractère distinctif*" permet de faire échapper la marque à la sanction de la déchéance.

En conséquence, tout laisse à penser que si les signes des marques en présence sont des plus proches (autrement dit, s'ils partagent le même caractère distinctif) l'usage d'une seule marque vaut usage de toutes les autres et fait donc échapper leur titulaire à la sanction de la déchéance.

Dans la pratique, les juges se sont montrés beaucoup plus nuancés, si ce n'est subtils.

La solution initiale

Par un arrêt du 16 juillet 1992[1], l'Assemblée plénière de la Cour de cassation a considéré que l'article L. 714-5 al. 2 b) CPI n'était applicable que dans la situation où la personne assignée en déchéance ne détenait qu'une seule marque enregistrée.

Autrement dit, l'opérateur économique qui avait procédé a l'enregistrement de plusieurs marques toutes constituées d'un signe semblable, mais qui n'en exploitait qu'une seule, encourrait la perte de toutes ses marques inutilisées ; l'usage de l'une ne valant pas
usage des autres, et ce en dépit de la proximité de leur signe.

Ainsi, les magistrats considérèrent dans l'affaire précitée que le titulaire de la marque enregistrée LOTUS ne pouvait se prévaloir de l'exploitation de sa marque AU LOTUS également enregistrée pour faire échapper la première à la déchéance.

Pour aboutir à cette solution, les juges ont estimé que celui qui prenait la peine de procéder à l'enregistrement de plusieurs marques, aussi proches soient-elles, manifestait de la sorte son intention de considérer que chacune d'elles était nécessairement dotée d'un caractère distinctif propre.

Si cette jurisprudence présentait, certes, le mérite de lutter contre les enregistrements abusifs de marques de barrage, elle rendait néanmoins, dans les autres cas, la position des titulaires de marques des plus délicates.

En effet, l'opérateur économique qui avait modernisé sa marque première sans procéder à l'enregistrement de son nouveau signe, précisément parce qu'il le considérait comme analogue à celui qu'il exploitait précédemment et qu'il souhaitait se prémunir de la jurisprudence LOTUS précitée, risquait, en cas de litige, de perdre tout droit de marque, dans l'éventualité où les juges considéraient que le signe second était différent de celui de la marque enregistrée.

La part de subjectivité dont est nécessairement empreinte la comparaison de deux signes afin de savoir s'ils partagent le même caractère distinctif instillait donc, dans ce contexte, une insécurité juridique difficilement tolérable, dans la mesure où elle était susceptible de démunir les titulaires de marques face aux contrefacteurs.

En outre, les juges ont rapidement compliqué la situation en introduisant de nouvelles distinctions dans leur construction jurisprudentielle.

Ainsi, une personne qui détenait deux marques enregistrées mais qui n'en exploitait qu'une seule pouvait néanmoins échapper à la déchéance si l'une de ses marques avait été acquise auprès d'un tiers dans la perspective de consolider les droits détenus sur l'autre marque…

On le mesure bien, la jurisprudence avait rendu l'appréciation de la validité des enregistrements parallèles de marques extrêmement délicate, si ce n'est subtile.

Les règles nouvelles

La Chambre commerciale de la Cour de cassation, par trois arrêts rendus le 14 mars 2006[2], a dit pour droit que l'article L. 714-5 al. 1 et 2 b) CPI "*exige seulement que la marque exploitée ne diffère de la marque enregistrée et non exploitée que par des éléments n'en altérant pas le caractère distinctif, peu important que la marque modifiée ait été elle-même enregistrée*" (nous soulignons).

Cette solution fut réaffirmée par un quatrième arrêt (émanant lui aussi de la Chambre commerciale de la Cour de cassation) rendu le 14 novembre 2006[3].

Dorénavant, la détention par la personne actionnée en déchéance de plusieurs marques enregistrées est donc devenue indifférente.

Cette solution présente de nombreux avantages tant juridiques que pratiques.

En effet, la position nouvellement adoptée par la Cour de cassation dans ces quatre décisions est plus fidèle de la lettre de l'article L 714-5 CPI, le texte ne distinguant pas selon que le signe (par hypothèse légèrement différent de celui de la marque objet de l'action en déchéance) dont la preuve de l'usage est apportée pour échapper à la déchéance est ou non enregistré à titre de marque.

En pratique, cette solution met également un terme à l'insécurité précédemment décrite dans laquelle se trouvaient les titulaires de marques.

En outre, cette nouvelle position de la Cour de cassation permet aux entreprises de considérer leurs marques non plus seulement comme des droits destinés à se défendre après la commission d'actes de contrefaçon, mais également comme de véritables armes permettant de gêner et donc de prendre l'avantage sur les concurrents dès leur dépôts.

Les arrêts rendus par la Cour de cassation légitimant la pratique décrite plus haut des marques de barrage, une entreprise semble donc dorénavant pouvoir accroître le périmètre de protection que lui confère la marque qu'elle exploite en déposant des marques similaires qui ne seront pas nécessairement utilisées.

De la sorte, cet opérateur économique pourra empêcher ses concurrents d'user de signes qui ne seraient pas similaires à la marque qu'elle exploite, mais qui le seraient à l'égard des variantes déposées, par hypothèse, non utilisées.

Une solution pérenne ?

Avant d'intégrer les enseignements des arrêts récemment rendus par la Cour de cassation dans les stratégies commerciales et juridiques, il convient néanmoins de se demander si les solutions dégagées sont viables et ont vocation à perdurer.

Il convient tout d'abord d'observer que les quatre décisions rompant avec la jurisprudence LOTUS de l'Assemblée plénière de la Cour de cassation, émanent certes de cette juridiction, mais plus précisément de sa chambre commerciale.

Il ne peut donc être exclu que les chambres civiles adoptent un avis différent.

En outre, valider la pratique des marques de barrage ne revient-elle pas à donner un blanc seing à une forme de pratique frauduleuse ?

En effet, de telles marques n'ont nullement pour but de désigner des produits ou des services dans la mesure où elles ne sont pas réellement utilisées sur le marché.

Par ailleurs, quelques jours après que les arrêts du 14 mars 2006 aient été rendus publics, le Tribunal de Première Instance des Communautés Européennes s'est prononcé pour la première fois sur la question de la licéité des enregistrements parallèles de marques et a adopté une position identique[4] à celle de l'Assemblée

plénière en 1992.

Certes, d'aucuns considéreront que le TPICE a statué en matière de marque communautaire et qu'il ne s'agit pas d'une décision comparable à celle que pourrait rendre la Cour de Justice des Communautés Européennes dans le cadre d'une saisine sur question préjudicielle.

Néanmoins, cette divergence de vue conduit à l'interrogation, d'autant que la décision du TPICE, si elle s'éloigne de la lettre des textes, n'en demeure pas moins conforme à leur esprit, ainsi qu'à la nature du droit de marque qui, comme nous l'avons évoqué, a vocation à être effectivement présent sur le marché.

En outre, le droit communautaire des marques est, sur le fond, identique au droit français des marques. Il y a donc là incompatibilité de solutions.

Cette incompatibilité est d'autant moins tolérable qu'elle risque de conduire à une distorsion de la concurrence, et donc à des pratiques susceptibles d'entrer en conflit avec le droit communautaire.

D'ailleurs, une discrimination est d'ores et déjà en train de se créer entre les justiciables des tribunaux français et ceux des instances communautaires.

En effet, selon qu'un titulaire de marque est attaqué en déchéance devant une juridiction française ou l'administration communautaire, la validité de ses enregistrements parallèles sera appréhendée différemment, puisque pour un magistrat français ceux-ci seront valables, alors que les mêmes ne le seront pas devant l'OHMI ou le TPICE qui statuerait à titre principal sur la déchéance.

Partant, une même situation juridique conduit à deux résultats diamétralement opposés.

Ceci est pour le moins paradoxal, dans la mesure où le droit communautaire (qu'il s'agisse de la Directive du 21 décembre 1988 rapprochant les législations des Etats membres sur les marques ou du Règlement 40/94 sur la marque communautaire) a précisément pour but de créer une certaine unité entre les différentes règles qui régissent le droit des marques.

Espérons donc que la Cour de Justice des Communautés Européennes (CJCE) soit rapidement appelée à clarifier la question.

A cet égard, si la décision dite BAINBRIDGE du TPICE fait actuellement l'objet d'un recours devant la CJCE, il n'est pas certain que la Cour soit amenée à se prononcer sur la licéité des marques de barrage.

En effet, dans ses conclusions, notamment aux points 72 et 86, l'Avocat général semble écarter la nécessité d'analyser juridiquement la question de savoir dans quelle mesure l'usage d'une marque enregistrée vaudrait usage d'une autre marque enregistrée, dès lors qu'en l'espèce le requérant ne rapporte la preuve de l'exploitation pour aucune des marques concernées[5].

Affaire à suivre…

Bruno RAIBAUT, Conseil en Propriété Industrielle
Fabrice BIRCKER, Juriste
CABINET DEGRET
cabinet.degret[AT]degret.com

[1] Cour de cassation, Assemblée plénière, 16 juillet 1992, pourvoi n° 89-16589

[2] Cour de cassation, Chambre commerciale, 14 mars 2006, pourvoi n° 04-10971, Cour de cassation, Chambre commerciale, 14 mars 2006, pourvoi n° 03-18732 et Cour de cassation, Chambre commerciale, 14 mars 2006, pourvoi n° 03-20198

[3] Cour de cassation, Chambre commerciale, 14 novembre 2006, pourvoi n° 04-15457

[4] Affaire T-194/03, 23 février 2006, Il Ponte Finanziaria SpA contre OHMI, BAINBRIDGE,

[5] Affaire C-234/06, Il Ponte Finanziaria,

R.D.T.I.C
LA REVUE DU DROIT DES TECHNIQUES DE L'INFORMATION ET DE LA COMMUNICATION-
N°6 3 – AVRIL 2007

INFORMATIQUE ET LIBERTÉS, VIE PRIVÉE

LA LOI RELATIVE À LA PRÉVENTION DE LA DÉLINQUANCE : DE NOUVELLES INTERCONNEXIONS DE DONNÉES PERSONNELLES À CARACTÈRE SOCIAL

Par Nicolas Samarcq

Publiée le 7 mars 2007, la loi relative à la prévention de la délinquance organise la transmission de données personnelles à caractère social entre les professionnels de l'action sociale

Publiée le 7 mars 2007, la loi relative à la prévention de la délinquance[1] organise la transmission de données personnelles à caractère social entre les professionnels de l'action sociale [2], le maire et le président du Conseil Général, l'institution d'un conseil pour les droits et devoirs des familles et la création d'un fichier communal d'assiduité scolaire.

La transmission des données sociales entre le maire, le président du Conseil Général et acteurs sociaux

L'article 8 de la loi relative à la prévention de la délinquance insère dans le Code de l'action sociale et des familles un nouvel article L. 121-6-2, qui définit le cadre dans lequel les professionnels de l'action sociale peuvent partager entre eux des informations confidentielles et les transmettre au maire ou au président du Conseil Général.

Le Conseil Constitutionnel, saisi sur le fondement du respect de la vie privée[3], a tout d'abord rappelé que le législateur a prévu, dans certaines hypothèses, de délier les intervenants de l'action sociale du secret professionnel afin de mieux prendre en compte l'ensemble des difficultés sociales, éducatives ou matérielles d'une personne ou d'une famille et de renforcer l'efficacité de l'action sociale, à laquelle concourt une coordination accrue de ces différents intervenants.

Le Conseil des sages a ensuite considéré, au regard du respect de la vie privée et des exigences de solidarité, que le législateur avait suffisamment encadré les modalités de transmission des données personnelles en prévoyant que :

- Un professionnel de l'action sociale doit transmettre des informations confidentielles au maire de la commune de résidence ou au président du Conseil Général que « *lorsque l'aggravation des difficultés sociales, éducatives ou matérielles d'une personne ou d'une famille appelle l'intervention de plusieurs professionnels* »[4] ;

- Les professionnels intervenant auprès d'une même personne ou d'une même famille, ainsi que le coordonnateur désigné par le maire, ont l'autorisation de « *partager entre eux des informations à caractère secret, afin d'évaluer leur situation, de déterminer les mesures d'action sociale nécessaires et de les mettre en œuvre* », dans la limite « *strictement nécessaire à l'accomplissement de la mission d'action sociale* »[5] ;

- Le professionnel agissant seul ou le coordonnateur sont autorisés à délivrer ces informations confidentielles au maire, au président du Conseil Général, ou à leur représentant[6] que si elles « *sont strictement nécessaires à l'exercice de leurs compétences* »[7] ;

- La communication de ces informations à des tiers est passible des peines prévues à l'article 226-13 du Code pénal [8].

Au regard de la loi Informatique et Libertés, l'ensemble de ces dispositions instituent de fait des échanges de données à caractère personnel, susceptibles de constituer un traitement automatisé de données sensibles soumis à autorisation préalable de la Commission Nationale Informatique et Libertés (CNIL).

En ce sens, la CNIL a rappelé, dans le cadre de son avis consultatif sur le projet de loi, que « *les traitements comportant des appréciations sur les difficultés sociales des personnes sont soumis à autorisation préalable de la Commission* » et doivent s'effectuer « *dans des conditions garantissant tout particulièrement la confidentialité des données* »[9].

Les élus devront donc prendre toutes précautions utiles pour garantir la confidentialité et la sécurité de ces données sensibles et certainement supprimer certaines d'entre elles lors des échanges. A défaut, leur demande d'autorisation pourra être refusée par la CNIL, qui a estimé que la communication au maire « *de l'ensemble des données relatives aux difficultés sociales de ses administrés, apparaissent, compte tenu de leur caractère très général, disproportionnées au regard des objectifs poursuivis* »[10]. En effet, selon le principe de proportionnalité de la loi Informatique et Libertés, les données collectées et traitées doivent être « *adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et de leurs traitements ultérieurs* »[11].

Le conseil pour les droits et devoirs des familles

Ce conseil, mis en place par délibération du conseil municipal, a pour mission de dialoguer avec les familles, leur adresser des recommandations et proposer des mesures d'accompagnement parental.

Ainsi, lorsqu'il ressort de constatations ou d'informations portées à la connaissance du Conseil que l'ordre, la sécurité ou la tranquillité publics sont menacés à raison du défaut de surveillance ou d'assiduité scolaire d'un mineur, le maire peut proposer aux parents ou au représentant légal du mineur concerné un accompagnement parental. Dans ce cas, le maire doit solliciter l'avis du président du Conseil Général, en informer l'inspecteur d'académie, le chef d'établissement d'enseignement, le directeur de l'organisme débiteur des prestations familiales et le préfet[12].

Le conseil pourra également proposer que les professionnels et les tiers concernés soient informés de ses recommandations et des engagements pris par la famille dans le cadre d'un contrat de responsabilité parentale signé avec le président du Conseil Général (ce contrat doit être porté à la connaissance du conseil pour les droits et devoirs des familles)[13].

Dans le cadre de l'avis précité, la CNIL a émis une réserve sur ce dispositif de signalement des mineurs et des familles à problèmes résidant dans la commune, dans la mesure où il a été institué sans qu'aucune garantie soit apportée « *ni sur l'origine des informations qui seraient utilisées pour procéder à ce signalement, ni sur les critères déclenchant ce signalement, ni sur les modalités de transmission et de traitement des informations et la nécessaire confidentialité de celles-ci* ». A titre d'exemple, les destinataires « tiers concernés » n'ont pas été définis par la loi.

En conséquent, les échanges de données nécessaires à la mise en place du Conseil pour les droits et devoirs des familles sont soumis à autorisation préalable de la CNIL, qui examinera avec vigilance les annexes « sécurités » et « échanges de données ».

Le fichier communal d'assiduité scolaire

Afin de procéder, chaque année (à la rentrée scolaire), au recensement des enfants résidant dans sa commune et qui sont soumis à l'obligation scolaire, le maire peut mettre en oeuvre un traitement automatisé de données à caractère personnel relatives aux enfants en âge scolaire, qui lui sont transmises par les organismes chargés du versement des prestations familiales, ainsi que par l'inspecteur d'académie ou le directeur de l'établissement d'enseignement.

Ce traitement enregistrera les avertissements prononcés par l'inspecteur d'académie aux personnes responsables d'enfants ayant manqué la classe sans motif légitime ni excuses valables au moins quatre demi-journées dans le mois.

Un décret en Conseil d'Etat, pris après avis de la CNIL, déterminera la liste des données à caractère personnel collectées, la durée de conservation de ces données, les modalités d'habilitation des destinataires ainsi que les conditions dans lesquelles les personnes intéressées peuvent exercer leur droit d'accès.

Conclusion

Il est donc à regretter que le législateur n'ait pas suivi les recommandations de la CNIL, notamment, en apportant les garanties nécessaires au respect des droits des personnes et en particulier de leur droit au respect de l'intimité de la vie privée des familles.

Désormais, la loyauté et la sécurité de ces traitements reposent sur la volonté politique et la sensibilisation des élus et agents en charge de l'action sociale et éducative.

Nicolas Samarcq
Juriste TIC
Membre de l'AFCDP (www.afcdp.org)
www.lexagone.com

[1] Loi n°2007-297 du 5 mars 2007 relative à la prévention de la délinquance, JORF du 7 mars 2007.

[2] Article L. 116-1 du Code de l'action sociale et des familles : « (…) l'Etat, les collectivités territoriales et leurs établissements publics, les organismes de sécurité sociale, les associations ainsi que par les institutions sociales et médico-sociales au sens de l'article L. 311-1. »

[3] Décision n° 2007-553 DC du 3 mars 2007 »Loi relative à la prévention de la délinquance ».

[4] Article L. 121-6-1 du Code de l'action sociale et des familles.

[5] Article L. 121-6-1 du Code de l'action sociale et des familles.

[6] au sens des articles L. 2122-18 et L. 3221-3 du Code général des collectivités territoriales.

[7] Article L. 121-6-1 du Code de l'action sociale et des familles.

[8] Article 226-13 du Code pénal : « *La révélation d'une information à caractère secret par une personne qui en est dépositaire soit par état ou par profession, soit en raison d'une fonction ou d'une mission temporaire, est punie d'un an d'emprisonnement et de 15000 euros d'amende* ».

[9] Délibération n°2006-167 du 13 juin 2006, www.cnil.fr/index.php?id=2089.

[10] Ibid.

[11] Article 6-3° de la loi Informatique et Libertés du 6 janvier 1978, modifiée le 6 août 2004.

[12] Article L. 141-2 du code de l'action sociale et des familles.

[13] Article L. 141-1 et L. 222-4-1 du code de l'action sociale et des familles.

R.D.T.I.C
LA REVUE DU DROIT DES TECHNIQUES DE L'INFORMATION ET DE LA COMMUNICATION-
N°6 3 – AVRIL 2007

Décret n° 2007-510 du 4 avril 2007 relatif à l'Autorité de régulation des mesures techniques instituée par l'article L. 331-17 du code de la propriété intellectuelle

NOR: MCCB0700270D

Le Premier ministre,

Sur le rapport du ministre de la culture et de la communication,

Vu la directive 2001/29/CE du Parlement européen et du Conseil du 22 mai 2001 sur l'harmonisation de certains aspects du droit d'auteur et des droits voisins dans la société de l'information ;

Vu le code pénal, notamment son article 432-12 ;

Vu le nouveau code de procédure civile, notamment le titre VI de son livre II ;

Vu le code de la propriété intellectuelle, notamment ses articles L. 331-5 à L. 331-22 ;

Vu le décret n° 92-681 du 20 juillet 1992 modifié relatif aux régies de recettes et aux régies d'avances des organismes publics ;

Vu le décret n° 2001-492 du 6 juin 2001 pris pour l'application du chapitre II du titre II de la loi n° 2000-321 du 12 avril 2000 et relatif à l'accusé de réception des demandes présentées aux autorités administratives ;

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

Décrète :

Article 1

Le chapitre Ier du titre III du livre III du code de la propriété intellectuelle (partie réglementaire) est modifié ainsi qu'il suit :

1° Il est créé une section 1, intitulée : « Dispositions communes », qui comprend l'article R. 331-1 ;

2° Il est créé une section 2 ainsi rédigée :

« Section 2 « Mesures techniques de protection et d'information

« Art. R. 331-2. - Les décisions prises par l'Autorité en application des règles de procédure prévues aux sous-sections 2, 3 et 4 de la présente section ne peuvent porter atteinte à l'exploitation normale d'une oeuvre ou d'un objet protégé par un droit de propriété intellectuelle, ni causer un préjudice injustifié aux intérêts légitimes des titulaires de droits de propriété intellectuelle.

« Sous-section 1 « Organisation et fonctionnement

de l'Autorité de régulation des mesures techniques

« Art. R. 331-3. - Les membres de l'Autorité sont convoqués par son président. La convocation est de droit à la demande du tiers des membres de l'Autorité. La convocation précise l'ordre du jour.

« L'Autorité ne peut valablement délibérer que si au moins trois de ses membres en exercice, avec voix délibérative, participent à la séance.

« Les séances de l'Autorité ne sont pas publiques.

« L'Autorité peut entendre toute personne dont l'audition lui paraît susceptible de contribuer à son information.

« Art. R. 331-4. - L'Autorité établit son règlement intérieur, qui précise notamment les conditions de son fonctionnement et les règles de déontologie ainsi que de procédure applicables devant elle.

« Art. R. 331-5. - Le président de l'Autorité est suppléé, en cas d'absence ou d'empêchement, par un membre qu'il désigne parmi les personnes mentionnées aux 1°, 2° et 3° de l'article L. 331-18.

« Le président de l'Autorité est remplacé, en cas de vacance, jusqu'à la nouvelle élection, par l'un des membres dans l'ordre prévu à l'article L. 331-18.

« Art. R. 331-6. - Le secrétaire général est désigné par l'Autorité, sur proposition de son président. Il prépare les délibérations de l'Autorité, met en oeuvre ses décisions et lui rend compte de l'exécution de celles-ci.

« Le président peut déléguer sa signature au secrétaire général pour signer tous actes relatifs au fonctionnement de l'Autorité.

« Des régies de recettes et d'avances peuvent être instituées conformément aux dispositions du décret n°

92-681 du 20 juillet 1992 relatif aux régies de recettes et aux régies d'avances des organismes publics.

« Art. R. 331-7. - Les rapporteurs sont nommés parmi les agents publics de catégorie A ou assimilés, en activité ou ayant fait valoir leurs droits à la retraite, et les personnes pouvant justifier d'une expérience d'au moins cinq ans dans le domaine du droit de la propriété intellectuelle ou dans celui des mesures techniques et titulaires d'un des diplômes permettant d'accéder à un corps de catégorie A.

« Peuvent également être nommés rapporteurs les magistrats de l'ordre judiciaire détachés ou mis à disposition de l'Autorité en application des dispositions de l'article R. 331-8.

« Art. R. 331-8. - Des fonctionnaires et des magistrats de l'ordre judiciaire peuvent être détachés ou mis à disposition auprès de l'Autorité dans les conditions prévues par leur statut.

« Le président de l'Autorité peut également faire appel, avec l'accord des ministres intéressés, aux services des ministères chargés de la culture, de la communication, de l'économie, des finances et de l'industrie, ainsi que du Centre national de la cinématographie, dont le concours est nécessaire à l'accomplissement de ses missions.

« Art. R. 331-9. - I. - L'Autorité fixe les règles de déontologie applicables à ses membres et rapporteurs, aux experts et à toute personne lui apportant son concours.

« II. - Les personnes mentionnées au I sont tenues au secret professionnel. Elles ne peuvent traiter une question dans laquelle elles ont un intérêt direct ou indirect. En cas de manquement à ces dispositions, l'Autorité statuant à la majorité de ses membres peut mettre fin à leur collaboration.

« III. - Les personnes mentionnées au I adressent au président de l'Autorité, à l'occasion de leur nomination ou de leur entrée en fonctions, une déclaration mentionnant leurs liens, directs ou indirects, avec toute société régie par le titre II du livre III du présent code ou toute entreprise exerçant une activité de production de phonogrammes ou de vidéogrammes, offrant des services de téléchargement ou tout titulaire de droits sur une mesure technique de protection et d'information. Cette déclaration doit être actualisée à leur initiative dès qu'une modification intervient concernant la nature ou l'étendue de ces liens, ou que de nouveaux liens sont noués.

« IV. - Lorsqu'un membre n'a pas assisté, sans motif valable, à cinq réunions consécutives du collège, l'Autorité peut, après que l'intéressé ait été préalablement invité à présenter ses observations, prononcer sa démission d'office. Le président en informe l'autorité qui a proposé la nomination de ce membre.

« Art. R. 331-10. - Le président de l'Autorité est rémunéré sous la forme d'indemnités forfaitaires mensuelles.

« Les membres de l'Autorité sont rémunérés sous la forme d'une indemnité forfaitaire par séance.

« Les rapporteurs et les personnes apportant leur concours à l'Autorité sont rémunérés sous la forme de vacations, dont le nombre est fixé par le président de l'Autorité, pour chaque dossier, en fonction du temps nécessaire à son instruction.

« Le montant et les modalités d'attribution de ces indemnités ainsi que le montant unitaire des vacations sont fixés par arrêté conjoint des ministres chargés de la culture, du budget et de la fonction publique.

« Les membres, les rapporteurs et les personnes apportant leur concours à l'Autorité peuvent prétendre au remboursement des frais de déplacement et de séjour que nécessite l'accomplissement de leurs missions, dans les conditions applicables aux personnels civils de l'Etat.

« Art. R. 331-11. - Lorsque l'Autorité est consultée par les commissions parlementaires, en application de l'article L. 331-17, sur les adaptations de l'encadrement législatif que nécessitent les évolutions dans le domaine des mesures techniques, son avis est rendu public.

« Le rapport de l'Autorité au Gouvernement et au Parlement, prévu à l'article L. 331-17, relatif aux évolutions constatées dans le domaine des mesures techniques et à leur impact prévisible sur la diffusion des contenus culturels, est également rendu public. Il comprend notamment les éléments de compte rendu mentionnés au troisième alinéa de cet article, s'agissant, d'une part, des décisions prises par l'Autorité, sur le fondement de l'article L. 331-7, en matière d'interopérabilité, d'autre part, des orientations qu'elle a fixées, dans le cadre des articles L. 331-8 à L. 331-16, pour ce qui regarde le périmètre et les modalités d'exercice de l'exception pour copie privée.

« Sous-section 2 « Règles générales

de procédure applicables devant l'Autorité

« Art. R. 311-12. - La saisine de l'Autorité fait l'objet d'une lettre recommandée avec demande d'avis de réception ou, selon des modalités fixées par l'Autorité, d'une transmission par voie électronique. Elle comporte au minimum :

« - le nom et l'adresse du demandeur, ainsi que, le cas

échéant, ses statuts et le mandat donné à son représentant ou à son conseil ;

« - les pièces justifiant que le demandeur relève de l'une des catégories de personnes autorisées à saisir l'Autorité en vertu des dispositions de la présente section ou des articles L. 331-7, L. 331-13 ou L. 331-14 ;

« - l'objet de la saisine, qui doit être motivée, et les pièces sur lesquelles se fonde celle-ci ;

« - le nom et, si le demandeur la connaît, l'adresse des parties que le demandeur met en cause.

« Lorsque l'Autorité est saisie en application des dispositions de l'article L. 331-7, le demandeur doit en outre préciser la nature et le contenu du projet dont la réalisation nécessite l'accès aux informations essentielles à l'interopérabilité qu'il sollicite, et justifier qu'il a demandé et s'est vu refuser cet accès, soit par le titulaire des droits sur la mesure technique, soit par le fournisseur, l'éditeur ou la personne procédant à l'importation ou au transfert des informations en cause depuis un Etat membre de la Communauté européenne. Est assimilé à un refus le fait de ne pas proposer cet accès à des conditions et dans un délai raisonnables.

« Si la saisine n'est pas accompagnée de ces éléments, une demande de régularisation est adressée au demandeur ou à son représentant mandaté, qui doivent y répondre et apporter les compléments dans un délai d'un mois.

« Le délai de deux mois mentionné aux articles L. 331-7 et L. 331-15 court à compter de la réception du dossier complet par l'Autorité.

« La production de mémoires, observations ou pièces justificatives effectuées par une partie devant l'Autorité sous la signature et sous le timbre d'un avocat emporte élection de domicile.

« Art. R. 331-13. - Sont regardées comme des personnes morales représentant les bénéficiaires des exceptions mentionnées à l'article L. 331-8, agréées pour saisir l'Autorité, en application de l'article L. 331-13, de tout différend portant sur les restrictions que les mesures techniques de protection apportent au bénéfice de ces exceptions :

« 1° Les associations de défense des consommateurs agréées en application des dispositions de l'article L. 411-1 du code de la consommation ;

« 2° Les associations agréées à cet effet par le ministre chargé de la culture.

« Art. R. 331-14. - L'agrément mentionné au 2° de l'article R. 331-13 est accordé pour une durée de cinq années aux associations qui remplissent les conditions suivantes à la date de la demande d'agrément :

« a) Justifier d'au moins trois années d'existence à compter de leur déclaration ;

« b) Justifier, pendant la période mentionnée à l'alinéa précédent, d'une activité effective et publique en vue de la défense des intérêts des bénéficiaires d'au moins l'une des exceptions mentionnées à l'article L. 331-8 ; cette activité est appréciée notamment en fonction de la réalisation et de la diffusion de publications et d'informations ;

« c) Réunir au moins cinquante membres cotisant individuellement, cette condition pouvant ne pas être exigée des associations se livrant à des activités de recherche et d'analyse de caractère scientifique ; lorsque l'association a une structure fédérale ou confédérale, il est tenu compte du nombre total de cotisants des associations la constituant.

« L'agrément est renouvelable dans les conditions de délivrance de l'agrément initial.

« Les demandes d'agrément et de renouvellement sont adressées au ministre chargé de la culture. La composition du dossier et les modalités d'instruction sont fixées par arrêté de ce ministre. Lorsque le dossier remis à l'administration est complet, il en est délivré récépissé dans les conditions prévues par le décret n° 2001-492 du 6 juin 2001. La décision d'agrément ou de refus est notifiée dans un délai de deux mois à compter de la délivrance du récépissé. Les décisions de refus doivent être motivées.

« Art. R. 331-15. - I. - L'Autorité peut rejeter pour irrecevabilité une demande dont elle a été saisie lorsque :

« 1° L'objet de la demande ne relève pas de sa compétence ;

« 2° La demande n'est pas conforme aux prescriptions de l'article R. 331-12, après l'expiration du délai d'un mois suivant l'invitation à régulariser qui a été adressée au demandeur ;

« 3° L'auteur de la saisine ne justifie pas d'une qualité ou d'un intérêt à agir.

« II. - L'Autorité peut statuer sans instruction sur les saisines entachées d'une irrecevabilité manifeste.

« Art. R. 331-16. - Le président peut, d'office ou à la demande des parties, procéder à la jonction de l'instruction de plusieurs affaires. A l'issue de leur instruction, l'Autorité peut se prononcer par une décision commune. Le président peut également procéder à la

disjonction de l'instruction d'une saisine en plusieurs affaires.

« Art. R. 331-17. - L'instruction de l'affaire s'effectue dans des conditions qui garantissent le respect du principe du caractère contradictoire de la procédure. Le président désigne le rapporteur. Celui-ci procède à toutes diligences utiles.

« La partie mise en cause est entendue à sa demande ou si le rapporteur l'estime utile. Le rapporteur peut également entendre toute autre personne dont l'audition lui paraît utile, notamment lorsqu'il est saisi d'une demande en ce sens par un tiers. Dans tous les cas, il établit un procès-verbal qui est versé au dossier.

« Le rapporteur peut verser au dossier les observations et pièces produites par des tiers. Il peut solliciter auprès des parties des pièces complémentaires et proposer de recourir à des expertises dans les conditions fixées à l'article R. 331-19.

« Art. R. 331-18. - I. - Lorsqu'une partie se prévaut d'un secret protégé par la loi, elle signale par lettre, à l'occasion de leur communication à l'Autorité, les informations, documents ou parties de documents regardés par elle comme mettant en jeu un secret protégé par la loi et demande, pour des motifs qu'elle précise pour chacun d'entre eux, leur classement en annexe confidentielle. Elle fournit séparément une version non confidentielle de ces documents ainsi qu'un résumé des éléments dont elle demande le classement. Le cas échéant, elle désigne les entreprises à l'égard desquelles le secret serait susceptible de s'appliquer.

« Lorsque les informations, documents ou parties de documents susceptibles de mettre en jeu un secret protégé par la loi sont communiqués à l'Autorité par une autre personne que celle qui est susceptible de se prévaloir de ce secret et que celle-ci n'a pas formé de demande de classement, le rapporteur l'invite à présenter, si elle le souhaite, dans un délai qu'il fixe, une demande de classement en annexe confidentielle conformément aux prescriptions de l'alinéa précédent.

« II. - Les informations, documents ou parties de documents pour lesquels une demande de classement n'a pas été présentée sont réputés ne pas mettre en jeu un secret protégé par la loi, notamment le secret des affaires, dont les parties pourraient se prévaloir.

« Le président de l'Autorité donne acte à la personne concernée du classement en annexe confidentielle des informations, documents ou partie de documents regardés par elle comme mettant en jeu un secret protégé par la loi. Les pièces considérées sont retirées du dossier ou certaines de leurs mentions sont occultées. La version non confidentielle des documents et leur résumé sont versés au dossier.

« Le président de l'Autorité peut refuser le classement en tout ou en partie si la demande n'a pas été présentée conformément aux dispositions du premier alinéa du présent article, ou l'a été au-delà des délais impartis en vertu du deuxième alinéa, ou si elle est manifestement infondée. La pièce est alors restituée à la partie qui l'a produite.

« III. - Lorsque le rapporteur considère qu'une pièce classée en annexe confidentielle est nécessaire à la procédure, il en informe par lettre recommandée avec accusé de réception la personne qui en a demandé le classement. Si cette personne s'oppose, dans le délai qui lui a été imparti par le rapporteur, à ce que la pièce soit utilisée dans la procédure, elle saisit le président de l'Autorité. Si celui-ci donne suite à son opposition, la pièce est restituée à la partie qui l'a produite. Dans le cas contraire, il autorise l'utilisation de la pièce par le rapporteur et sa communication aux parties pour lesquelles la pièce est nécessaire à l'exercice de leurs droits. Les parties concernées ne peuvent utiliser cette pièce, qui demeure couverte par le secret protégé par la loi, que dans le cadre de la procédure devant l'Autorité et des voies de recours éventuelles contre les décisions de celle-ci.

« Lorsqu'une partie considère qu'une pièce classée en annexe confidentielle est nécessaire à l'exercice de ses droits, elle peut en demander la communication ou la consultation en présentant une requête motivée au rapporteur. Le rapporteur informe la personne qui a demandé le classement de cette pièce par lettre recommandée avec accusé de réception. Si cette dernière s'oppose, dans le délai qui lui a été imparti par le rapporteur, à ce que la pièce soit communiquée à la partie qui en fait la demande, elle saisit le président de l'Autorité. Si celui-ci donne suite à son opposition, la pièce est restituée à la partie qui l'a produite. Dans le cas contraire, il autorise la communication ou la consultation de la pièce à la partie qui en a fait la demande ainsi que, le cas échéant, aux autres parties pour lesquelles la pièce est nécessaire à l'exercice de leurs droits. Les parties concernées ne peuvent utiliser cette pièce, qui demeure couverte par le secret protégé par la loi, que dans le cadre de la procédure devant l'Autorité et des voies de recours éventuelles contre les décisions de celle-ci.

« IV. - Les décisions prises par le président de l'Autorité en application des dispositions du présent article ne peuvent être contestées qu'à l'occasion du recours dirigé contre les décisions de l'Autorité rendues en application des articles R. 331-22 à R. 331-24 et R. 331-27.

« Art. R. 331-19. - Les experts mentionnés à l'article L. 331-20 sont désignés par le président de l'Autorité sur proposition du rapporteur chargé de l'instruction de l'affaire. La décision du président définit l'objet de

l'expertise, fixe le délai de sa réalisation et évalue les honoraires prévisibles correspondants.

« Les honoraires et frais d'expertise sont à la charge de la partie qui en a fait la demande ou à celle de l'Autorité, dans le cas où l'expertise est ordonnée d'office par le président sur proposition du rapporteur. Toutefois, l'Autorité peut, dans sa décision sur le fond, faire peser tout ou partie de la charge définitive de l'expertise sur certaines parties dans les conditions prévues à l'article R. 331-28.

« Lorsqu'une expertise est demandée par une partie et acceptée par le président, le montant d'une provision égale aux honoraires prévus par l'expert est consigné sur demande du président. Si plusieurs parties doivent procéder à une telle consignation, le président indique dans quelle proportion chacune doit consigner.

« Le rapport d'expertise est remis au rapporteur chargé de l'instruction de l'affaire, qui le verse au dossier.

« Sous-section 3 « Procédure applicable

en matière d'interopérabilité des mesures techniques

« Art. R. 331-20. - Lorsque le rapporteur constate que les engagements proposés par chacune des parties recueillent l'accord de l'ensemble de celles-ci et qu'ils sont de nature à mettre un terme aux pratiques contraires à l'interopérabilité au sens des dispositions de l'article L. 331-7, il établit un projet de procès-verbal signé par les parties en cause, constatant ces engagements et fixant un délai pour leur exécution. Ce procès-verbal devient définitif après accord de l'Autorité, qui peut entendre les parties ou toute autre personne avant de statuer si elle le juge utile.

« Les engagements mentionnés à l'alinéa précédent peuvent être modifiés avec l'accord de l'Autorité selon la procédure prévue à cet alinéa.

« Art. R. 331-21. - I. - A défaut d'accord des parties et de l'Autorité constaté dans les conditions fixées par l'article R. 331-20, le rapport du rapporteur est notifié aux parties, qui disposent d'un délai de quinze jours pour prendre connaissance et copie du dossier auprès des services de l'Autorité et pour transmettre à celle-ci leurs observations écrites.

« Lorsque les circonstances le justifient, le président de l'Autorité peut, par une décision non susceptible de recours, accorder un délai supplémentaire, qui ne peut excéder un mois, pour la consultation du dossier et la production des observations des parties.

« Les parties sont informées de la date à laquelle l'Autorité statuera sur la saisine au moins dix jours avant la séance. La personne mise en cause est entendue à sa demande ou à celle du président de l'Autorité. Elle doit pouvoir prendre la parole en dernier.

« L'Autorité peut également entendre le demandeur ou toute personne dont l'audition lui paraît utile.

« Les personnes entendues peuvent être assistées d'un conseil.

« Le rapporteur qui a instruit une affaire peut présenter des observations orales lors de la séance au cours de laquelle elle est examinée. L'Autorité statue hors de sa présence.

« Lorsqu'elle estime que l'instruction est incomplète, l'Autorité peut décider de renvoyer l'affaire en tout ou partie à l'instruction. Cette décision n'est pas susceptible de recours.

« II. - L'Autorité peut, si elle le juge utile, demander à son président de saisir pour avis le Conseil de la concurrence selon les modalités fixées au dernier alinéa de l'article L. 331-7 et décider de surseoir à statuer, dans l'attente de cet avis, sur la demande dont elle a été saisie.

« Art. R. 331-22. - I. - Au terme de la procédure prévue à l'article R. 331-21, l'Autorité peut, par une décision motivée, soit rejeter la demande dont elle a été saisie, soit enjoindre au titulaire des droits sur la mesure technique de prendre les mesures propres à assurer l'accès du demandeur aux informations essentielles à l'interopérabilité.

« Lorsqu'elle prononce une injonction, l'Autorité définit les conditions d'accès à ces informations, notamment :

« 1° La durée de cet accès et son champ d'application ;

« 2° L'indemnité que le demandeur doit verser au titulaire des droits sur la mesure technique, lorsque celui-ci présente une demande justifiée à cette fin. L'injonction prend effet au plus tôt à la date de versement de l'indemnité à celui-ci ou à la date de consignation de cette somme selon des modalités fixées par l'Autorité. Le montant de cette indemnité tient compte notamment de la valeur économique des informations communiquées au demandeur.

« L'Autorité précise en outre les engagements que le demandeur doit respecter pour garantir, d'une part, l'efficacité et l'intégrité de la mesure technique, et, d'autre part, les conditions d'utilisation du contenu protégé et les modalités d'accès à celui-ci. Ces engagements peuvent comporter l'obligation de faire vérifier par un expert désigné par l'Autorité que l'efficacité et l'intégrité de la mesure technique sont respectées. Ces engagements portent également sur les conditions de publication du

code source et de la documentation technique en application des dispositions du troisième alinéa de l'article L. 331-7, lorsque le demandeur déclare à l'Autorité vouloir publier ces éléments.

« II. - L'Autorité peut assortir cette injonction d'une astreinte dont elle fixe le montant et la date d'effet. Lorsque l'Autorité constate, à compter de cette date, d'office ou sur la saisine de toute partie intéressée, que les mesures qu'elle avait prescrites n'ont pas été prises, elle procède à la liquidation de l'astreinte. Celle-ci est provisoire ou définitive. Elle doit être considérée comme provisoire, à moins que l'Autorité n'ait précisé son caractère définitif. L'Autorité peut modérer ou supprimer l'astreinte provisoire, même en cas d'inexécution constatée.

« Art. R. 331-23. - Lorsque aucun recours devant la cour d'appel de Paris n'a été formé dans le délai prévu au premier alinéa de l'article R. 331-28 ou lorsque ce recours a été rejeté par une décision juridictionnelle devenue définitive, l'Autorité peut, à la demande de toute partie intéressée, modifier ou mettre fin à son injonction si des éléments nouveaux le justifient ou si le demandeur renonce à donner suite à sa demande d'accès aux informations en litige. L'Autorité statue, au terme de la procédure prévue aux articles R. 331-12 à R. 331-19 et R. 331-21, selon les modalités fixées à l'article R. 331-22.

« Art. R. 331-24. - En cas de non-respect des engagements acceptés par l'Autorité suivant la procédure fixée à l'article R. 331-20 ou en cas d'inexécution de l'injonction prononcée en application des dispositions des articles R. 331-22 et R. 331-23, le demandeur mentionné à ces articles peut saisir l'Autorité afin que celle-ci prononce à l'encontre du titulaire des droits sur la mesure technique la sanction pécuniaire prévue à l'article L. 331-7.

« Cette sanction pécuniaire peut également être prononcée, à la demande du titulaire des droits sur la mesure technique, à l'encontre du demandeur si celui-ci ne respecte pas soit les engagements qu'il a pris et qui ont été acceptés par l'Autorité suivant la procédure fixée à l'article R. 331-20, soit les engagements qui lui ont été imposés par l'Autorité en application des dispositions du I de l'article R. 331-22.

« L'Autorité statue au terme de la procédure prévue aux articles R. 331-12 à R. 331-19 et R. 331-21.

« Art. R. 331-25. - Le rapporteur peut demander au titulaire des droits sur la mesure technique ou, dans le cas prévu au deuxième alinéa de l'article R. 331-24, au demandeur, de lui communiquer, dans un délai de dix jours, les montants de chiffres d'affaires nécessaires au calcul du plafond d'une éventuelle sanction. Si la partie concernée s'abstient de lui communiquer ces informations ou s'il conteste l'exactitude de celles-ci, le rapporteur indique dans son rapport son évaluation des chiffres d'affaires en cause et les éléments sur lesquels il fonde celle-ci.

« Sous-section 4 « Procédure applicable en matière d'exceptions

au droit d'auteur et aux droits voisins

« Art. R. 331-26. - Lorsque le rapporteur constate qu'une conciliation des parties est possible en application des dispositions du premier alinéa de l'article L. 331-15, il établit un projet de procès-verbal signé par les parties en cause, constatant la conciliation, précisant les mesures à prendre pour mettre fin à la situation litigieuse et fixant un délai pour l'exécution de ces mesures. Ce procès-verbal de conciliation devient définitif et exécutoire après accord de l'Autorité, qui peut entendre les parties avant de statuer si elle le juge utile.

« Le procès-verbal est déposé immédiatement au secrétariat-greffe du ou des tribunaux d'instance dans le ressort duquel ou desquels les parties au litige ont leur domicile ou siège social.

« Toute conciliation réalisée ultérieurement est constatée par procès-verbal établi et déposé dans les mêmes conditions.

« Art. R. 331-27. - En cas d'échec de la conciliation, l'Autorité peut, par une décision motivée prise au terme de la procédure fixée par le I de l'article R. 331-21, soit rejeter la demande dont elle a été saisie, soit enjoindre à la personne mise en cause de prendre les mesures propres à assurer le bénéfice effectif de l'exception au droit d'auteur ou aux droits voisins. Elle détermine alors les modalités d'exercice de cette exception et fixe notamment, le cas échéant, le nombre minimal de copies autorisées dans le cadre de l'exception pour copie privée, en fonction du type d'oeuvre ou d'objet protégé, des divers modes de communication au public et des possibilités offertes par les techniques de protection disponibles.

« L'Autorité peut assortir cette injonction d'une astreinte selon les modalités prévues au II de l'article R. 331-22.

« Sous-section 5 « Voies de recours contre les décisions

de l'Autorité de régulation des mesures techniques

« Art. R. 331-28. - Les décisions de l'Autorité mentionnées aux articles R. 331-22 à R. 331-24 et R. 331-27 sont notifiées par lettre recommandée avec

demande d'avis de réception aux parties, qui peuvent, dans le délai d'un mois, introduire un recours en annulation ou en réformation devant la cour d'appel de Paris. Les augmentations de délais prévues à l'article 643 du nouveau code de procédure civile ne s'appliquent pas à ce recours.

« La lettre de notification doit indiquer le délai de recours ainsi que les modalités selon lesquelles celui-ci peut être exercé. Elle comporte en annexe les noms, qualités et adresses des parties auxquelles la décision de l'Autorité a été notifiée. Les délais de recours ne sont pas opposables à l'auteur de celui-ci lorsque la lettre de notification ne comporte pas les indications prévues au présent alinéa.

« Ces décisions ainsi que les procès-verbaux mentionnés aux articles R. 331-20 et R. 331-26 sont rendus publics par tous moyens et, en tout état de cause, s'agissant des décisions, au Bulletin officiel du ministère de la culture et de la communication. L'Autorité peut prévoir une publication limitée pour tenir compte de l'intérêt légitime des parties à ce que leurs secrets protégés par la loi ne soient pas divulgués. Une copie de ces documents est adressée au ministre chargé de la culture et, pour ce qui concerne les litiges relatifs à l'interopérabilité des mesures techniques, au ministre chargé de la propriété industrielle.

« L'Autorité peut mettre tout ou partie des frais de procédure à la charge du demandeur dont la demande est rejetée ou à celle de la personne mise en cause lorsqu'une injonction ou une sanction pécuniaire est prononcée à son encontre. Ces frais incluent, le cas échéant, le coût de l'expertise mentionnée à l'article R. 331-19 et celui de la publication de la décision.

« Les sanctions pécuniaires et les astreintes sont recouvrées comme les créances de l'Etat étrangères à l'impôt et au domaine.

« Art. R. 331-29. - Par dérogation aux dispositions du titre VI du livre II du nouveau code de procédure civile, les recours exercés devant la cour d'appel de Paris contre les décisions de l'Autorité sont formés, instruits et jugés conformément aux dispositions de la présente sous-section.

« L'Autorité n'est pas partie à l'instance.

« Art. R. 331-30. - Les recours prévus à l'article R. 331-28 sont formés par une déclaration écrite en triple exemplaire déposée contre récépissé au greffe de la cour d'appel de Paris contenant, à peine de nullité :

« 1° Si le demandeur est une personne physique, ses nom, prénoms, profession et domicile ; si le demandeur est une personne morale, sa dénomination, sa forme, son siège social et l'organe qui la représente ;

« 2° L'objet du recours.

« Lorsque la déclaration ne contient pas l'exposé des moyens invoqués, le demandeur doit, à peine d'irrecevabilité prononcée d'office, déposer cet exposé au greffe dans les deux mois qui suivent la notification de la décision de l'Autorité.

« La déclaration de recours mentionne la liste des pièces et documents justificatifs produits. Les pièces et documents mentionnés dans la déclaration sont remis au greffe de la cour d'appel en même temps que la déclaration. Le demandeur au recours joint à la déclaration une copie de la décision attaquée.

« Lorsque le demandeur au recours n'est pas représenté, il doit informer sans délai le greffe de la cour de tout changement de domicile.

« Art. R. 331-31. - Dans les cinq jours qui suivent le dépôt de sa déclaration, l'auteur du recours doit, à peine d'irrecevabilité de ce dernier prononcée d'office, en adresser, par lettre recommandée avec demande d'avis de réception, une copie aux parties auxquelles la décision de l'Autorité a été notifiée, ainsi qu'il ressort de la lettre de notification prévue au deuxième alinéa de l'article R. 331-28.

« Dès l'enregistrement du recours, le greffe de la cour d'appel notifie une copie de la déclaration mentionnée à l'article R. 331-30 et des pièces qui y sont jointes au président de l'Autorité, ainsi qu'au ministre chargé de la culture et, pour ce qui concerne les litiges relatifs à l'interopérabilité des mesures techniques, au ministre chargé de la propriété industrielle.

« Le président de l'Autorité transmet au greffe de la cour le dossier de l'affaire qui comporte le rapport, les mémoires et pièces transmis par les parties et tous les documents versés au dossier durant l'instruction.

« Art. R. 331-32. - Un recours incident peut être formé alors même que son auteur serait forclos pour exercer un recours à titre principal. Toutefois, dans ce dernier cas, le recours incident ne sera pas recevable s'il est formé plus d'un mois après la réception de la lettre recommandée de l'auteur du recours formé à titre principal, prévue au premier alinéa de l'article R. 331-31, ou si le recours principal n'est pas lui-même recevable.

« Le recours incident est formé selon les modalités prévues à l'article R. 331-30. Il est dénoncé, dans les conditions prévues au premier alinéa de l'article R. 331-31, à l'auteur du recours à titre principal.

« Art. R. 331-33. - Lorsque le recours risque d'affecter les droits ou les charges d'autres personnes qui étaient parties en cause devant l'Autorité, ces personnes

peuvent se joindre à l'instance devant la cour d'appel par déclaration écrite et motivée déposée au greffe dans les conditions prévues à l'article R. 331-30, dans le délai d'un mois après la réception de la lettre recommandée de l'auteur du recours formé à titre principal, prévue au premier alinéa de l'article R. 331-31. Elle est notifiée à l'auteur du recours formé à titre principal.

« A tout moment, le premier président ou son délégué ou la cour peut mettre d'office en cause ces mêmes personnes. Le greffe notifie la décision de mise en cause par lettre recommandée avec demande d'avis de réception.

« Art. R. 331-34. - Le premier président de la cour d'appel ou son délégué fixe les délais dans lesquels les parties à l'instance doivent se communiquer leurs observations écrites et en déposer copie au greffe de la cour. Il fixe également la date des débats.

« Le greffe notifie ces délais aux parties et les convoque à l'audience par lettre recommandée avec demande d'avis de réception.

« Art. R. 331-35. - Les notifications entre parties ont lieu par lettre recommandée avec demande d'avis de réception ou par notification directe entre les avocats ou les avoués des parties. Les pièces de procédure doivent être déposées au greffe en triple exemplaire.

« Art. R. 331-36. - Devant la cour d'appel ou son premier président, la représentation et l'assistance des parties s'exercent dans les conditions prévues par l'article 931 du nouveau code de procédure civile.

« Art. R. 331-37. - Les décisions de la cour d'appel de Paris ou de son premier président sont notifiées par lettre recommandée avec demande d'avis de réception par le greffe de la cour aux parties à l'instance.

« Elles sont portées à la connaissance du président de l'Autorité, du ministre chargé de la culture et, pour ce qui concerne les litiges relatifs à l'interopérabilité des mesures techniques, au ministre chargé de la propriété industrielle, par lettre simple à l'initiative du greffe. »

Article 2

Le présent décret est applicable à Mayotte, dans les îles Wallis et Futuna, dans les Terres australes et antarctiques françaises et en Nouvelle-Calédonie.

Article 3

Le ministre de l'économie, des finances et de l'industrie, le garde des sceaux, ministre de la justice, le ministre de la culture et de la communication, le ministre de l'outre-mer et le ministre délégué à l'industrie 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 4 avril 2007.

Dominique de Villepin

Par le Premier ministre :

Le ministre de la culture

et de la communication,

Renaud Donnedieu de Vabres

Le ministre de l'économie,

des finances et de l'industrie,

Thierry Breton

Le garde des sceaux, ministre de la justice,

Pascal Clément

Le ministre de l'outre-mer,

Hervé Mariton

Le ministre délégué à l'industrie,

François Loos

DROIT-TIC .com

R.D.T.I.C

LA REVUE DU DROIT DES TECHNIQUES DE L'INFORMATION ET DE LA COMMUNICATION-N°6 3 – AVRIL 2007

AVIS DE LA COMMISSION GÉNÉRALE DE TERMINOLOGIE ET DE NÉOLOGIE, 20 avril 2007

Vocabulaire de l'informatique (liste de termes, expressions et définitions adoptés), J.O du 15 décembre 2006, n° 290, p. 18979.

NOR : CTNX0609644X

« I. - Termes et définitions

antémémoire, n.f.
Domaine : Informatique.
Synonyme : mémoire cache.
Définition : Mémoire très rapide, intercalée entre le processeur et la mémoire principale, que l'ordinateur consulte avant d'interroger la mémoire principale et qui, fournissant les parties de programme et les données les plus utilisées dans le traitement en cours, permet de réduire la durée de celui-ci.
Note : La capacité de l'antémémoire est un des éléments déterminants de la puissance de l'ordinateur.
Voir aussi : cache.
Équivalent étranger : cache memory, cache storage.
Attention : Cette publication annule et remplace celle des termes « mémoire d'accès rapide » et « antémémoire » au Journal officiel du 22 septembre 2000.

cache, n.m.
Domaine : Informatique.
Définition : Mémoire ou partie de mémoire dans laquelle sont stockés de façon temporaire les données ou les programmes les plus fréquemment ou les plus récemment utilisés, que l'ordinateur peut interroger afin de réduire les temps de réponse.
Note : Parmi les caches les plus utilisés, on trouve les antémémoires ou mémoires caches, les caches situés sur disque, ceux destinés à améliorer les performances des disques eux-mêmes (cache-disque), ainsi que des zones de la mémoire principale qu'occupent certains logiciels.
Équivalent étranger : cache.

cache-disque, n.m.
Domaine : Informatique.
Définition : Cache, intercalé entre le processeur et le disque, qui évite une lecture sur le disque auquel l'accès serait plus lent.
Voir aussi : cache.
Équivalent étranger : disk cache.

cache-toile, n.m.
Domaine : Informatique.
Définition : Cache qui contient temporairement une copie des documents consultés récemment et qui permet à l'utilisateur d'en disposer sans qu'il soit nécessaire de procéder à une nouvelle recherche sur la toile.
Note : On dit que les documents concernés sont « mis en cache ».
Voir aussi : cache.
Équivalent étranger : web cache.

centre d'assistance
Domaine : Informatique.
Définition : Service chargé de répondre aux demandes d'assistance émanant des utilisateurs de produits ou de services.
Note : Suivant le degré d'urgence et le niveau de difficulté, le centre d'assistance peut apporter une réponse, donner un conseil, transmettre le problème à un spécialiste.
Voir aussi : numéro d'urgence, téléassistance.
Équivalent étranger : help desk.

entrepôt de données
Domaine : Informatique.
Définition : Ensemble de données collectées dans une entreprise ou un organisme pour être exploitées par des outils d'aide à la décision.
Équivalent étranger : data warehouse.

fournisseur d'applications en ligne
Domaine : Informatique.
Synonyme : fournisseur de services d'applications.
Définition : Prestataire qui offre à plusieurs clients la possibilité d'utiliser la même application informatique à travers un réseau de télécommunication afin d'en répartir le coût.
Équivalent étranger : application service provider (ASP).

fournisseur de services d'applications
Domaine : Informatique.
Voir : fournisseur d'applications en ligne.

gant numérique
Domaine : Informatique.
Définition : Gant muni de capteurs destinés à convertir les mouvements de la main et des doigts en signaux utilisables par un ordinateur pour l'analyse de gestes ou l'action dans un environnement de synthèse.
Équivalent étranger : data glove.

gérance de l'informatique
Domaine : Informatique.
Définition : Prise en charge contractuelle de tout ou partie de la gestion d'un système d'information d'un organisme par un prestataire extérieur.
Note : On trouve aussi, dans le langage professionnel, le terme « infogérance », qui n'est pas recommandé.
Équivalent étranger : facilities management.
Attention : Cette publication annule et remplace celle du Journal officiel du 10 octobre 1998.

implémenter, v. (langage professionnel)
Domaine : Informatique.
Définition : Effectuer l'ensemble des opérations qui permettent de définir un projet et de le réaliser, de l'analyse du besoin à l'installation et la mise en service du système ou du produit.
Voir aussi : implanter.
Équivalent étranger : implement (to).

interface, n.f.
Domaine : Informatique-Télécommunications.
Définition : Limite physique ou théorique entre deux systèmes matériels ou logiciels, entre deux parties d'un système ou entre l'utilisateur et sa machine, où s'appliquent les règles et conventions régissant leur interaction ; par extension, l'ensemble de ces règles et conventions.
Note : Les règles et conventions concernent notamment des caractéristiques physiques (mécaniques, électriques, optiques...), des caractéristiques de signaux, des caractéristiques sémantiques ou fonctionnelles, des échanges d'information.
Équivalent étranger : interface.

logiciel d'enseignement
Domaine : Informatique.
Voir : logiciel éducatif.
Attention : Cette publication annule et remplace celle des termes « logiciel pédagogique » et « logiciel éducatif » au Journal officiel du 22 septembre 2000.

logiciel de traitement de texte
Forme abrégée : traitement de texte.
Domaine : Informatique.
Définition : Logiciel permettant de créer, de modifier et de mettre en forme des documents en vue de les conserver, de les transmettre ou de les imprimer.
Note :
1. Au sens strict, l'expression « traitement de texte » désigne l'action de créer et de manipuler des documents. Dans l'usage courant, cette expression désigne aussi le logiciel.
2. On trouve parfois, dans le langage professionnel, le terme « texteur », qui n'est pas recommandé.
Voir aussi : traitement de texte.
Équivalent étranger : word processor.

logiciel éducatif
Domaine : Informatique.
Synonyme : logiciel d'enseignement.
Définition : Logiciel d'aide à l'acquisition de connaissances ou de compétences.
Note :
1. Un logiciel éducatif peut comporter un module de contrôle des connaissances acquises par l'utilisateur.
2. On trouve aussi, dans le langage professionnel, le terme « didacticiel ».
Équivalent étranger : educational software.
Attention : Cette publication annule et remplace celle des termes « logiciel pédagogique » et « logiciel éducatif » au Journal officiel du 22 septembre 2000.

logiciel gratuit
Domaine : Informatique.
Définition : Logiciel que l'auteur met à la disposition des utilisateurs sans exiger de rémunération, mais en conservant l'intégralité de ses droits.
Équivalent étranger : freeware.

logiciel libre
Domaine : Informatique.
Définition : Logiciel distribué avec l'intégralité de ses programmes-sources, afin que l'ensemble des utilisateurs qui l'emploient puissent l'enrichir et le redistribuer à leur tour.
Note : Un logiciel libre n'est pas nécessairement gratuit et les droits de la chaîne des auteurs sont préservés.
Équivalent étranger : free software, open-source software.

macrocommande, n.f.
Domaine : Informatique.
Voir : script.

mémoire cache
Domaine : Informatique.
Voir : antémémoire.
Attention : Cette publication annule et remplace celle des termes « mémoire d'accès rapide » et « antémémoire » au Journal officiel du 22 septembre 2000.
modèle, n.m.
Domaine : Informatique.
Note :
1. Les éditeurs de logiciels fournissent souvent des modèles pour faciliter l'utilisation de leurs produits, par exemple : un prototype de facture dans un logiciel de traitement de texte, ou bien une déclaration-type d'ajout d'utilisateurs dans un outil de gestion de réseau.
2. Un modèle général peut servir à créer d'autres modèles, répondant à des usages spécifiques.
Équivalent étranger : template.

réalité de synthèse
Domaine : Informatique.
Définition : Environnement créé à l'aide d'un ordinateur et donnant à l'utilisateur la sensation d'être immergé dans un univers artificiel.
Note :
1. La création d'une réalité de synthèse nécessite des dispositifs d'entrée-sortie particuliers tels des gants numériques, un visiocasque, un système de restitution sonore évolué, etc., associés à des logiciels graphiques tridimensionnels.
2. On trouve aussi, dans l'usage courant, la locution « réalité virtuelle », qui n'est pas recommandée.
Équivalent étranger : virtual reality.

recherche en texte intégral
Domaine : Informatique.
Définition : Recherche de mots, de phrases ou d'une chaîne de caractères quelconque dans un ensemble de documents, s'appuyant sur une exploration systématique de la totalité de cet ensemble.
Note : La recherche en texte intégral peut s'effectuer aussi bien dans le document original que sur un résumé ou un document dérivé, tel que notice ou table des matières, et elle ne porte pas seulement sur un ensemble restreint de mots clés.
Équivalent étranger : full-text search.

relationnel, -elle, adj.
Domaine : Informatique.
Définition : Se dit d'une base de données construite sur un modèle fondé sur la théorie mathématique des relations.
Note : Dans ce modèle, dit « relationnel », les données sont stockées en tables structurées sous une forme qui facilite les manipulations et permet d'éviter la redondance de l'information que l'on rencontre dans des modèles plus anciens.
Équivalent étranger : relational.

réseautique, n.f.
Domaine : Informatique-Télécommunications.
Définition : Ensemble des activités et des techniques destinées à créer, gérer, exploiter et utiliser des réseaux de télécommunication ou des réseaux d'ordinateurs.
Équivalent étranger : networking.
Attention : Cette publication annule et remplace celle du terme « mise en réseau » au Journal officiel du 10 octobre 1998.

script, n.m.
Domaine : Informatique.
Synonyme : macrocommande, n.f.
Définition : Programme constitué d'une suite de commandes dispensant l'utilisateur de les saisir, et permettant d'effectuer une fonction particulière ou de contribuer à l'exécution d'un autre programme.
Note :
1. Un script peut être notamment un programme associé à un document décrit à l'aide d'un langage de balisage et destiné à améliorer l'interactivité.
2. Le terme « macrocommande » est souvent abrégé en « macro », n.f.
Équivalent étranger : macro, macrocommand, script.

serveur, n.m.
Domaine : Informatique.
Définition : Matériel, logiciel ou système informatique destiné à fournir un service déterminé à d'autres systèmes informatiques ou à des utilisateurs connectés sur un réseau.
Note : Exemples : serveur de bases de données, serveur d'impression, serveur de messagerie.
Équivalent étranger : server.
Attention : Cette publication annule et remplace celle du Journal officiel du 16 mars 1999 et du Journal officiel du 22 septembre 2000.

surcadencer, v.
Domaine : Informatique.
Définition : Faire fonctionner un processeur à une cadence supérieure à celle pour laquelle il a été initialement conçu, afin d'en améliorer les performances.
Équivalent étranger : overclock (to).

tutoriel, n.m.
Domaine : Informatique.
Définition : Guide d'initiation et d'aide à l'utilisation d'un produit ou d'un service informatique.
Équivalent étranger : tutorial. »

DROIT-TIC .com

R.D.T.I.C

LA REVUE DU DROIT DES TECHNIQUES DE L'INFORMATION ET DE LA COMMUNICATION-
N°6 3 – AVRIL 2007

DÉLIBÉRATION CNIL

Dél. n° 2006-281 du 14 décembre 2006 sanctionnant la société Tyco healthcare France

Thèmes
Informatique et libertés, responsabilité
Abstract
CNIL, contrôle sur place, fichier international de gestion des ressources humaines, communication d'informations erronées (oui), mise en demeure (oui), articles 45 et suivants de la loi du 6 janvier 1978, sanction pécuniaire (oui)
Résumé
Mise en demeure de faire la lumière sur la mise en œuvre d'un fichier international de gestion des ressources humaines, la société Tyco Healthcare France a communiqué à la CNIL des informations erronées
Décision

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

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 personne ;

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 ;

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°2006-147 du 23 mai 2006 fixant le règlement intérieur de la Commission nationale de l'informatique et des libertés ;

Vu la délibération n° 2006-144 adoptée par la CNIL le 10 mai 2006 ;

Vu la décision de mission de contrôle n° 2006-074C ;

Vu le rapport de M. Emmanuel de GIVRY, commissaire, notifié à la société Tyco Healthcare France le 27 octobre 2006 et les observations en réponse reçues le 24 novembre 2006.

Après avoir entendu, lors de la réunion du 14 décembre 2006, M. Emmanuel de GIVRY, commissaire, en son rapport et Mme Pascale COMPAGNIE, commissaire du Gouvernement, en ses observations.

Après avoir entendu, lors de la réunion du 14 décembre 2006, les observations orales de Maître LORELEI, avocat, représentant la société Tyco Healthcare France, celle-ci ayant pris la parole en dernier.

Constate les faits suivants :

1. La société Tyco Healthcare France a déclaré à la CNIL le 22 septembre 2004 un traitement de données ayant pour finalité la « gestion des carrières à l'international ».

Par courrier en date du 21 février 2005, la CNIL lui a demandé de lui faire parvenir certains éléments d'information indispensables à l'instruction de ce dossier. La société Tyco Healthcare France n'a apporté aucune suite satisfaisante aux demandes de la Commission réitérées dans ses courriers des 19 septembre 2005 et 21 mars 2006.

En effet, la réponse adressée par la société Tyco Healthcare France SAS le 4 avril 2006 n'a pas permis d'apporter les réponses à l'ensemble des questions formulées par les services de la CNIL dans le cadre de l'instruction du dossier de déclaration (le descriptif précis des finalités exactes recherchées, les cas précis dans lesquels des données à caractère personnel sont envoyées en Grande-Bretagne et aux Etats-Unis, les lieux exacts d'implantation des serveurs et des systèmes, les fonctionnalités précises de l'application, les destinataires exacts des données, les mesures de sécurité assurant la confidentialité des données et la durée de conservation des données).

2. Au regard des faits précités, la Commission a, par délibération adoptée le 10 mai 2006, mis en demeure la société Tyco, sous dix jours, de répondre aux questions posées par la CNIL dans ses courriers (courriers des 21 février, 19 septembre 2005, 21 mars 2006) ou de lui indiquer que le traitement précité avait été abandonné.

3. En réponse à la mise en demeure, la société Tyco Healthcare France a indiqué, par courrier du 1er juin 2006, que : « Le groupe Tyco au niveau international devait scinder les 4 secteurs d'activités qui le constituent actuellement en entités indépendantes. Cette scission doit intervenir d'ici la fin de l'année calendaire. Par conséquent les procédures et les demandes

d'information qui avaient été mises en place sont dans les circonstances actuelles suspendues ».

4. La CNIL ne s'estimant pas suffisamment informée par cette réponse sur le sort exact ayant été finalement réservé au traitement objet de la mise en demeure a fait procéder à une mission de contrôle sur place le 12 juillet 2006 dans les locaux de la société Tyco Healthcare France.

A cette occasion, les services de la CNIL ont constatée que le traitement objet de la mise en demeure, contrairement à ce qui avait été affirmé, était bien utilisé par la société Tyco Healthcare France.

Au regard des documents communiqués (« International Database Project Update, Data Auditing and Next Steps, June 2006 » et « Guide de l'administrateur, Administration et traitement des données pour la base de données internationales »), le traitement précité apparaît comme un outil de gestion essentiel, au plan mondial, de la politique salariale du groupe Tyco dont les finalités dépassent largement la finalité de « reporting » visée dans la déclaration du 22 septembre 2004. Lors de la mission de contrôle sur place, il a également été constaté que de strictes et récentes procédures étaient mises en œuvre pour que la société Tyco Healthcare France alimente de façon régulière la base de données avec les informations concernant les salariés français.

5. Il ressort de ce qui précède que les faits constatés sur place le 12 juillet 2006 étaient en contradiction avec la réponse adressée par la société Tyco Healthcare France le 1er juin 2006 puisque celle-ci n'a ni « suspendu » la mise en œuvre du traitement objet de la mise en demeure ni répondu à l'ensemble des questions posées concernant les modalités exactes de fonctionnement du traitement précité.

En effet, s'agissant tout d'abord du descriptif précis des finalités recherchées et des fonctionnalités de l'application, dans son courrier du 4 avril 2006 la société Tyco Healthcare France indique que « la finalité de cette base de données est purement celle d'un « reporting » vis à vis de notre hiérarchie européenne en ressources humaines ».

Un document interne datant de juin 2006 communiqué aux services de la CNIL lors de la mission de contrôle du 12 juillet 2006 indique pourtant (« International Database Project Update, Data Auditing and Next Steps, June 2006 »), concernant le traitement précité, que celui-ci sert à la gestion des stock-options, la formation professionnelle, le niveau des rémunérations, la communication professionnelle, etc. Lors de la réunion du 14 décembre 2006, l'avocat représentant la société Tyco Healthcare France a également indiqué oralement que le traitement objet de la mise en œuvre avait également pour finalité de gérer la « mobilité interne ».

Dès lors, la Commission ne s'estime toujours pas informée sur le descriptif précis des finalités recherchées par le traitement déclaré le 22 septembre 2004 par la société Tyco Healthcare France comme cela était pourtant demandé dans la mise en demeure du 10 mai 2006.

S'agissant ensuite des cas précis dans lesquels des données à caractère personnel sont envoyées dans les locaux du groupe Tyco en Grande-Bretagne et aux Etats-Unis, le courrier du 4 avril 2006 se limite à indiquer que « ces données peuvent être transmises du Royaume-Uni aux Etats-Unis si notre hiérarchie juge opportun de le faire ».

Si le contrôle du 12 juillet 2006 a permis d'établir une communication d'informations concernant le traitement objet de la mise en demeure entre la société Tyco Healthcare France et les locaux du groupe Tyco en Angleterre et aux Etats-Unis, il n'a pas été possible d'obtenir des informations précises sur les motifs liés à cet envoi d'informations.

Dès lors, la Commission ne s'estime toujours pas correctement informée des cas précis où des données à caractère personnel sont envoyées dans les locaux du groupe Tyco en Grande-Bretagne et aux Etats-Unis comme cela était pourtant demandé dans la mise en demeure du 10 mai 2006.

S'agissant encore des lieux exacts d'implantation des serveurs et des systèmes, seul un schéma technique a été communiqué aux services de la Commission (« Schéma de fonctionnement informatique Tyco Healthcare France ») mais les adresses exactes des centres informatiques n'ont pas été communiquées à ce jour.

S'agissant des questions posées concernant les destinataires exacts des données et la durée de conservation des données, la Commission ne dispose à ce jour d'aucune réponse précise.

S'agissant enfin des mesures de sécurité assurant la confidentialité des données, si la mission de contrôle du 12 juillet 2006 a permis d'établir que l'accès aux ordinateurs de la société Tyco Healthcare France est sécurisé par mot de passe, la Commission ne dispose à ce jour d'aucune information technique précise sur les conditions de sécurité liées à la conservation des données en Angleterre et aux Etats-Unis.

Dès lors, la Commission ne s'estime toujours pas correctement informée sur les lieux exacts d'implantation

des serveurs et des systèmes, les destinataires exacts des données, la durée de conservation des données et les mesures de sécurité assurant la confidentialité des données comme cela était pourtant demandé dans la mise en demeure du 10 mai 2006.

6. Dans ses observations en réponse du 24 novembre 2006 et lors de la réunion du 14 décembre 2006, la société Tyco Healthcare France soutient que la proposition de sanction proposée par le rapporteur serait mal fondée sur le plan juridique dans la mesure où celle-ci ne s'appuierait sur aucune mise en demeure préalable mais uniquement sur la réalisation de la mission de contrôle du 12 juillet 2006.

Sur ce point, la Commission observe qu'une procédure de sanction peut être engagée lorsque le responsable d'un traitement ne se conforme pas à la mise en demeure qui lui est adressée (article 45 de la loi du 6 janvier 1978 modifiée le 6 août 2004). La présente procédure de sanction s'appuie ainsi sur la mise en demeure prononcée par la CNIL le 10 mai 2006 et sur la réponse adressée par la société Tyco le 1er juin 2006.

Il convient par ailleurs de rappeler que dans le cadre de l'analyse de la réponse adressée par la société Tyco le 1er juin 2006, la CNIL était en droit de procéder à une mission de vérification sur place afin, de vérifier la réalité des informations qui lui avaient été communiquées. La Commission estime à cet égard que les informations transmises par la société Tyco Healthcare France dans son courrier du 1er juin 2006 ne permettaient pas de connaître le sort exact ayant été réservé au traitement objet de la mise en demeure du 10 mai 2006.

Au surplus, la société Tyco Healthcare France relève dans ses observations du 24 novembre 2006 que la décision de mission de contrôle n° 2006-074C ne visait pas formellement la mise en demeure du 10 mai 2006. Sur ce point, la Commission estime que l'existence d'une procédure de mise en demeure n'a, à cet égard, aucune incidence sur le formalisme à respecter pour la réalisation d'une telle mission de contrôle.

La Commission considère par conséquent que la procédure de sanction est pleinement régulière.

7. La société Tyco a par ailleurs fait valoir dans ses observations du 24 novembre 2006 et lors de la réunion du 14 décembre 2006 que les informations communiquées lors de la mission de contrôle ne concerneraient pas le même traitement que celui visé dans la mise en demeure du 10 mai 2006.

La Commission observe que les vérifications opérées sur place le 12 juillet 2006 par les services de la CNIL ont permis de constater que le traitement déclaré par la société Tyco Healthcare France le 22 septembre 2004 (« gestion des carrières à l'international »), comportait, comme indiqué précédemment, d'autres fonctionnalités relatives à la gestion des ressources humaines telles que par exemple la gestion des stock-options, la formation professionnelle, le niveau des rémunérations, la communication professionnelle ainsi que la mobilité interne.

Ces fonctionnalités, qui peuvent être rattachées à une finalité de gestion des carrières à l'international, n'étaient pas décrites dans la déclaration adressée par la société Tyco Healthcare France le 22 septembre 2004.

La Commission observe par ailleurs que les captures d'écran réalisées par les services de la CNIL lors du contrôle du 12 juillet 2006 sont concordantes s'agissant des catégories de données collectées et utilisées avec les « champs » informatiques figurant dans la déclaration adressée par la société Tyco Healthcare France le 22 septembre 2004 (données démographiques concernant les salariés, données sur la situation administrative des salariés, données concernant la localisation géographique des salariés, données sur la rémunération des salariés, etc.).

Dès lors, la Commission considère que les vérifications opérées par la CNIL le 12 juillet 2006 concernaient bien le traitement visé dans la mise en demeure du 10 mai 2006.

8. Il ressort de l'ensemble de ce qui précède que la société Tyco Healthcare France ne s'est pas conformée à la mise en demeure de la CNIL du 10 mai 2006 puisqu'elle n'a pas communiqué les éléments demandés par la CNIL concernant le traitement déclaré le 22 septembre 2004 (le descriptif précis des finalités exactes recherchées, le cas précis dans lesquels des données à caractère personnel sont envoyées en Grande-Bretagne et aux Etats-Unis, les lieux exacts d'implantation des serveurs et des systèmes, les fonctionnalités précises de l'application, les destinataires exacts des données, les mesures de sécurité assurant la confidentialité des données et la durée de conservation des données) et qu'elle n'a pas cessé la mise en œuvre de celui-ci.

La Commission observe à cet égard que la société Tyco Healthcare France n'a manifestement pas pris la mesure de la gravité des manquements qui lui sont reprochés concernant son manque de coopération et de transparence.

En conséquence, la Commission décide de faire application des dispositions des articles 45 et suivants de la loi du 6 janvier 1978 modifiée le 6 août 2004 et de prononcer à l'encontre de la société Tyco Healthcare France sise 2 rue Denis Diderot, La clef de Saint Pierre à Elancourt (78), compte tenu de la gravité des

manquements commis, une sanction pécuniaire de 30.000 euros.

Par ailleurs, la Commission enjoint la société Tyco Healthcare France de répondre, sous dix jour à compter de la notification de la présente délibération, à l'ensemble des demandes formulées par la CNIL dans sa mise en demeure du 10 mai 2006.

La présente décision sera rendue publique.

Le président, Alex Türk

Référence : CNIL, 14 décembre 2006, *N° 2006-281 SANCTIONNANT LA SOCIÉTÉ TYCO HEALTHCARE FRANCE*, DROIT-TIC
http://www.droit-tic.com/juris/aff.php?id_juris=94

(1) L'échantillon total s'est réduit du fait des décès, des départs à l'étranger et des pertes de contact avec les intéressés, notamment à la suite d'un déménagement.

Référence : CNIL, 08 février 2007, *N° 2007-022 AUTORISANT L'INSTITUT NATIONAL DE LA STATISTIQUE ET DES ÉTUDES ÉCONOMIQUES À METTRE EN OEUVRE LES TRAITEMENTS AUTOMATISÉS DE DONNÉES À CARACTÈRE PERSONNEL NÉCESSAIRES À LA RÉALISATION ET À L'EXPLOITATION DES RÉSULTATS D'UNE ENQUÊTE STATISTI*, DROIT-TIC
http://www.droit-tic.com/juris/aff.php?id_juris=93

DROIT-TIC .com

R.D.T.I.C

LA REVUE DU DROIT DES TECHNIQUES DE L'INFORMATION ET DE LA COMMUNICATION-
N°6 3 – AVRIL 2007

Dél. n° 2007-021 du 8 février 2007 autorisant à titre expérimental, pendant un an, la mise en œuvre par la société RIA France d'un traitement automatisé des ordres de transfert internationaux de fonds ayant notamment pour finalité la lutte contre le blanchiment de capitaux...

Thèmes
Informatique et libertés, Droit pénal

Résumé
autorisant à titre expérimental, pendant un an, la mise en oeuvre par la société RIA France d'un traitement automatisé des ordres de transferts internationaux de fonds ayant notamment pour finalité la lutte contre le blanchiment de capitaux...

Décision

COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTES - CNIL

Délibération 2007-021 du 08 février 2007

Délibération autorisant à titre expérimental, pendant un an, la mise en oeuvre par la société RIA France d'un traitement automatisé des ordres de transferts internationaux de fonds ayant notamment pour finalité la lutte contre le blanchiment de capitaux et le financement du terrorisme.

La Commission nationale de l'informatique et des libertés,
Vu la Convention n° 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;
Vu la directive 91/308/CE du Conseil du 10 juin 1991 modifiée relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ;
Vu la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement de données à caractère personnel et la libre circulation de ces données ;
Vu le règlement n° 1781/2006 du Parlement européen et du Conseil du 15 novembre 2006 relatif aux informations concernant le donneur d'ordre accompagnant les virements de fonds ;
Vu la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée par la loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, et notamment ses articles 25-1-4° et 69 ;
Vu le code monétaire et financier, notamment ses articles L. 511-34, L. 561-1 à L. 563-5, L. 574-1, L. 574-2, L. 613-13, R. 562-1, R. 562-2, R. 563-1 à R. 563-3 et R. 564-1 ;
Vu le décret n° 2005-1309 du 20 octobre 2005 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 précitée ;
Vu le dossier déposé par la société en cours de constitution Ria France relatif à un traitement automatisé de données personnelles ayant pour finalité la saisie et la transmission des ordres de transfert de fonds internationaux ;

Après avoir entendu M. Philippe NOGRIX, commissaire, en son rapport, et Mme Pascale COMPAGNIE, commissaire du Gouvernement, en ses observations,

Formule les observations suivantes :

La société financière Ria France a saisi la Commission nationale de l'informatique et des libertés le 24 octobre 2006 d'un dossier relatif à la mise en oeuvre d'un traitement de données à caractère personnel dont la finalité principale est d'assurer la saisie et le routage d'ordres de transfert de fonds internationaux entre particuliers, vers des pays et au bénéfice de populations faiblement bancarisés.

Ce traitement automatisé intègre, notamment, un dispositif de lutte contre le blanchiment d'argent et le financement du terrorisme qui vise à détecter les opérations qui sont susceptibles, du fait des anomalies qu'elles comportent, d'être qualifiées d'infraction de blanchiment par les autorités compétentes. De ce fait, ces opérations peuvent donner lieu, après la collecte de renseignements complémentaires, à l'envoi d'informations au ministère de l'économie, des finances et de l'industrie, soit au bureau de la direction générale du Trésor et de la politique économique (DGTPE) en charge du mécanisme de gel des avoirs, soit au service d'analyse du renseignement financier Tracfin sous la forme de déclarations de soupçon.

La détection de ces opérations avant leur réalisation peut conduire la banque à suspendre la transaction engagée par le client sur la base de contrôles intégralement automatisés, notamment après consultation de liste des personnes faisant l'objet de sanctions financières, dont certaines n'ont pas force de loi sur le territoire national. Ce traitement peut ainsi conduire à exclure des personnes du bénéfice d'une prestation en l'absence de toute disposition légale applicable en France prévoyant la mise en oeuvre d'une telle exclusion. Dès lors, il relève du 4° du I de l'article 25 de la loi du 6 janvier 1978 modifiée et doit être autorisé par la CNIL.

Les données enregistrées dans le traitement concernent les nom, prénoms, date de naissance, adresse et numéro de téléphone du client, les type, pays d'émission, numéro et date d'expiration de la pièce d'identité présentée, le montant de l'opération projetée, la devise

fournie et la devise de reversement, les coordonnées complètes du bénéficiaire du paiement, le pays dans lequel le décaissement doit avoir lieu, la banque correspondante choisie sur une liste et l'adresse de réception du transfert. Le document d'identité présenté - de type carte d'identité, passeport ou carte de séjour - est scanné. Pour les clients réguliers, le système informatique permet de récupérer les renseignements déjà enregistrés.

Des filtres informatisés sont mis en place, qui suspendent automatiquement le traitement des demandes d'opérations lorsque : elles excèdent certains montants fixés dans l'agrément de Ria France ; elles se rapportent à des personnes susceptibles de figurer sur des listes officielles des personnes faisant l'objet d'une sanction financière internationale ; elles ne sont pas complètement renseignées ; la pièce d'identité présentée n'est plus valable.

Les listes de sanctions financières internationales prises en considération sont, d'une part, celles applicables en France, qu'elles soient mises en oeuvre au niveau national, au niveau européen ou qu'elles soient imposées par l'ONU, d'autre part, celles que l'OFAC (office of Foreign Assets Control, administration relevant du département du Trésor américain), est chargé de faire respecter et que le groupe américain Ria est tenu d'appliquer.

Les opérations ainsi suspendues sont soumises à un réexamen, le plus souvent après collecte d'informations complémentaires auprès du client sur le motif du transfert, l'origine des fonds transférés, son activité professionnelle et son employeur, en vue d'une levée de la mesure ou d'un rejet définitif de l'ordre par le responsable anti-blanchiment.

La Commission prend acte que le contrôle renforcé mis à la charge de l'établissement en cas de concordance entre l'identité d'un client et un signalement sur l'une de ces listes précitées garantit que les opérations de transfert ne seront définitivement bloquées qu'en présence d'indices sérieux et concordants et que le service de lutte anti-blanchiment ou de gel des avoirs compétent - la DGTPE ou l'OFAC - sera rendu destinataire de données personnelles concernant ce client.

Elle note également que l'ensemble des données personnelles recueillies par Ria France dans le cadre d'une demande de transfert de fonds lui permet de s'assurer que les vérifications, après suspension de l'ordre de transfert, sont effectuées très rapidement, au plus tard dans les 24 à 48 heures.

Elle relève que les personnes ayant déjà fait l'objet d'une suspension d'ordre de virement pour cause d'homonymie feront l'objet d'un signalement informatique spécifique, accessible aux seuls agents chargés de la lutte anti-blanchiment, qui permettra de régler plus rapidement tout nouveau blocage de leurs opérations.

Dès lors, le traitement mis en place est conforme à l'intérêt légitime du responsable du traitement sans méconnaître pour autant l'intérêt des clients concernés.
L'ensemble des informations saisies est transmis, via le réseau sécurisé du groupe Ria, au centre informatique de la société Ria Envia Inc., situé en Californie où sont assurés le traitement automatisé de l'ordre et son re-routage vers le pays de destination de l'ordre, chez le correspondant désigné par le client lors de la saisie de l'ordre de transfert.

La Commission observe que les États-Unis ne font pas, à ce jour, partie des Etats reconnus comme disposant d'une législation garantissant un niveau de protection suffisant de la vie privée et des libertés et droits fondamentaux des personnes à l'égard du traitement des données à caractère personnel.

Conformément à l'avant-dernier alinéa de l'article 69 de la loi du 6 janvier 1978 modifiée, la Commission a compétence pour autoriser tout transfert de données à caractère personnel envisagé vers cet Etat, dès lors que le traitement effectué par le destinataire sur ces données garantit un niveau de protection suffisant de la vie privée ainsi que des libertés et droits fondamentaux des personnes, notamment en raison des conditions contractuelles ou règles internes dont il fait l'objet.

A cet égard, la Commission constate que la société Ria Envia Inc. a adhéré à la "sphère de sécurité" ("Safe Harbour"). En outre, Ria France et Ria Envia Inc. s'engagent à signer un avenant à leur convention de gestion, qui précise les conditions d'utilisation des informations auxquelles Ria Envia Inc. aura accès en qualité de support technique ou au titre de la lutte anti-blanchiment. Ce document rappelle que Ria France répond, en qualité de responsable du traitement, aux demandes de divulgation des données personnelles qui lui seraient adressées par des autorités étrangères dans le cadre des dispositions du droit national en vigueur, notamment en ce qui concerne le secret professionnel.

La transmission aux États-Unis des données nécessaires au routage des ordres de virement est, à cet égard, adéquate, pertinente et non excessive au regard des finalités poursuivies. La Commission estime qu'il n'en va pas de même de la transmission des copies scannées des pièces d'identité des clients de Ria France, aux seules fins de leur archivage, qui ne parait pas s'imposer au regard des conditions envisagées à l'article 69 pour justifier des transferts de données personnelles vers des pays n'assurant pas un niveau de protection suffisant.
En conséquence, la Commission demande au groupe Ria d'envisager une autre solution technique que la transmission des copies scannées des pièces d'identité

des clients de Ria France, aux seules fins de leur archivage, aux États-Unis, qui pourrait consister dans l'organisation de l'archivage des documents scannés en Espagne, pays servant de base logistique au groupe Ria en Europe.

Les données enregistrées, sont destinées à être conservées pendant cinq ans, conformément au règlement européen du 15 novembre 2006 susvisé.

Les destinataires des informations traitées sont :
- les agents habilités de Ria France, notamment en charge de la lutte anti-blanchiment, de la conformité et du contrôle interne,
- ceux de l'organisme correspondant chargé du versement des fonds dans le pays de destination (sauf pour les copies scannées des documents d'identité),
- à titre temporaire, les services de la filiale espagnole du groupe Ria qui assurent un rôle de formation et d'accompagnement au moment de la mise en place d'une fonction anti-blanchiment en France,
- les membres de l'équipe anti-blanchiment (Compliance officer) de la société mère américaine qui bénéficient d'une autorisation expresse, pour les données relatives aux transactions faisant l'objet d'une déclaration à l'OFAC.

En outre, des informations pourront être transmises, dans le cadre de leurs compétences respectives :
- au service Tracfin, dans le cadre de l'application du dispositif de lutte contre le blanchiment de l'argent, notamment dans le cas où l'identité du donneur d'ordre ou du bénéficiaire reste douteuse malgré les diligences effectuées,
- au bureau de la DGTPE chargé du mécanisme de gel des avoirs, pour les seules données relatives aux personnes qui font l'objet d'une mesure de gel des avoirs pour leurs liens présumés avec une activité terroriste,
- à l'OFAC, pour les seules données relatives aux donneurs d'ordre ou aux bénéficiaires des opérations qui figurent effectivement sur les listes en vigueur de l'OFAC et les données relatives aux virements de fonds les concernant.

Les clients sont informés sur les reçus qui leur sont donnés à chaque opération des finalités des traitements mis en oeuvre par Ria, des destinataires des données personnelles, ainsi que des modalités d'exercice des droits d'accès et de rectification.

Dans ces conditions, la Commission autorise à titre expérimental, pour une durée limitée à un an, Ria France SAS à mettre en oeuvre le traitement de données personnelles présenté. Elle demande, en outre, qu'avant l'expiration de ce délai, lui soit adressée une nouvelle demande d'autorisation comportant notamment un rapport concernant le nouveau dispositif d'archivage des pièces d'identité ainsi qu'un bilan portant sur l'évaluation et l'évolution du dispositif de lutte anti-blanchiment mis en place et sur les transmissions de données en résultant.
Le Président, Alex TURK.

Référence : CNIL, 08 février 2007, *2007-021 AUTORISANT À TITRE EXPÉRIMENTAL, PENDANT UN AN, LA MISE EN OEUVRE PAR LA SOCIÉTÉ RIA FRANCE D'UN TRAITEMENT AUTOMATISÉ DES ORDRES DE TRANSFERTS INTERNATIONAUX DE FONDS AYANT NOTAMMENT POUR FINALITÉ LA LUTTE CONTRE LE BLANCHIMENT DE CAPITAUX...*, DROIT-TIC
http://www.droit-tic.com/juris/aff.php?id_juris=98

DROIT-TIC .com

R.D.T.I.C

LA REVUE DU DROIT DES TECHNIQUES DE L'INFORMATION ET DE LA COMMUNICATION-
N°6 3 – AVRIL 2007

Dél. n° 2007-041 du 8 mars 2007 portant autorisation de la mise en œuvre par ADP d'un traitement de données à caractère personnel reposant sur la reconnaissance par empreinte digitales et ayant pour finalité le contrôle de l'accès...

Thèmes
Informatique et libertés, Droits de la personnalité
Résumé
Délibération portant autorisation de la mise en oeuvre par Aéroports de Paris d'un traitement automatisé de données à caractère personnel reposant sur la reconnaissance des empreintes digitales et ayant pour finalité le contrôle de l'accès
Décision

COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTES - CNIL

Délibération 2007-041 du 08 mars 2007

Délibération portant autorisation de la mise en oeuvre par Aéroports de Paris d'un traitement automatisé de données à caractère personnel reposant sur la reconnaissance des empreintes digitales et ayant pour finalité le contrôle de l'accès au sein de la zone réservée du satellite S3 de l'aéroport de Paris-Charles-de-Gaulle.

La Commission nationale de l'informatique et des libertés,
Vu la Convention n° 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;
Vu la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement de données à caractère personnel et la libre circulation de ces données ;
Vu la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée par la loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, notamment son article 25-8° ;
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 demande d'autorisation, présentée par Aéroports de Paris, d'un traitement automatisé de données à caractère personnel reposant sur la reconnaissance des empreintes digitales et ayant pour finalité le contrôle de l'accès au sein de la zone réservée du satellite S3 de l'Aéroport de Paris-Charles-de-Gaulle ;
Après avoir entendu M. Hubert Bouchet, commissaire en son rapport et Mme Pascale Compagnie, commissaire du Gouvernement, en ses observations.

Formule les observations suivantes :

La Commission nationale de l'informatique des libertés a été saisie par la société Aéroports de Paris (ADP) le 2 février 2007 d'un dossier de formalité préalable relatif à la mise en oeuvre d'un traitement automatisé de données à caractère personnel reposant sur la reconnaissance des empreintes digitales et ayant pour finalité le contrôle de l'accès au sein de la zone réservée du satellite S3 de l'Aéroports de Paris-Charles-de-Gaulle.

Il y a lieu de faire application des dispositions prévues à l'article 25-8° de la loi du 6 janvier 1978 modifiée qui soumet à autorisation les traitements comportant des données biométriques nécessaires au contrôle de l'identité des personnes.

Le dispositif présenté par Aéroports de Paris a pour finalité le contrôle de l'accès à certaines zones ou locaux situées en zone réservée sécurité du nouveau satellite d'embarquement appelé S3 dont l'ouverture est prévue entre les mois de juin et octobre 2007. Il est dans une large mesure identique à celui déjà utilisé pour le contrôle de l'accès aux autres zones réservées sécurité des aéroports de Paris-Charles-de-Gaulle et d'Orly et qui a fait l'objet d'un avis favorable de la CNIL par sa délibération n° 04-017 du 8 avril 2004.

Les traitements envisagés ont pour objet d'autoriser l'accès de certains locaux ou zones du satellite aux seules personnes ayant une justification professionnelle. En fonction du niveau de sensibilité de la zone ou des locaux, le processus de contrôle d'accès est le suivant :
- lecture d'un badge délivrés par la Direction Générale de l'Aviation Civile (DGAC) dans le cadre de la gestion des activités de sûreté sur les plates-formes aéroportuaires ;
- vérification en temps réel des droits d'accès associés à ce badge en interrogeant une base de données ;
- authentification de la personne grâce à un dispositif de reconnaissance des empreintes digitales.

La phase relative à la vérification des droits d'accès associés au badge repose sur l'interrogation d'un serveur central dans lequel sont enregistrés les données relatives aux personnes concernées (le nom, le prénom, le type d'activité, l'entreprise ayant délivré l'accréditation, l'entreprise d'appartenance, le numéro de badge et la date de fin de validité de badge).

Certains personnels habilités de la société Air France, compagnie opérant sur le satellite S3, de la société ADP, ainsi que de la Direction de la Police aux Frontières disposent d'un accès, en consultation et en alimentation,

à cette base de données afin de gérer, en fonction des zones et des locaux, les habilitations de leurs propres personnels. Les personnes habilités auront uniquement accès aux données des employés de leur organisme. Cet aspect du dispositif constitue l'une des principales différences avec le système de contrôle d'accès mis en oeuvre dans les autres parties de l'aéroport de Paris-Charles-de-Gaulle et qui a fait l'objet de la délibération n° 04-017 précitée.

S'agissant du procédé de reconnaissance des empreintes digitales, l'authentification des personnes s'effectuera localement par une lecture du gabarit des empreintes digitales exclusivement enregistrés, sous forme chiffrée, dans la puce sans contact des badges délivrés par la DGAC. Le contrôle d'accès s'effectuera par une comparaison entre le doigt apposé sur le lecteur et le gabarit de l'empreinte digitale enregistré sur le badge.

Un historique des passages, le détail des accès empruntés ainsi que la liste des irrégularités pourront être édités. La conservation de ces données ne pourra excéder trois mois et elle seront uniquement accessibles aux administrateurs et personnels en charge de la maintenance des serveurs d'ADP.

Les données relatives au profil des personnes concernées seront conservées dans le serveur central jusqu'à expiration de la date de validité du badge. Il en est de même pour le gabarit enregistré sur le badge.
L'information des personnels se fera au moyen de la remise d'un document lors de l'opération d'accréditation ainsi que par un affichage dans les salles où cette procédure aura lieu. Une information et une consultation du comité d'entreprise de la société Aéroports de Paris seront effectués.

Compte tenu de l'impératif de sécurité lié à la nécessité de contrôler l'accès aux zones réservées de l'aéroport de Paris-Charles-de-Gaulle et dans la mesure où il repose sur l'enregistrement du gabarit de l'empreinte digitale dans un support individuel exclusivement détenu par la personne concernée, le traitement apparaît, en l'état actuel des connaissances sur la technologie utilisée, adapté et proportionné à la finalité assignée au dispositif.
Les droits d'accès et de rectification s'exerceront auprès du pôle gestion du patrimoine - activités domaniales - direction de l'aéroport de Paris-Charles-de-Gaulle - BP 24101 - 97711 Roissy Charles de Gaulle cedex.
Les catégories de données à caractère personnel enregistrées seront :
- dans la base de données gérée par les organismes opérant sur le satellite S3 : le nom, le prénom, le type d'activité, l'entreprise ayant délivré l'accréditation, l'entreprise d'appartenance, le numéro de badge et la date de fin de validité de badge ainsi que l'historique des passages, le détail des accès empruntés et la liste des irrégularités ;
- dans les badges : le gabarit des empreintes digitales, le code PIN associé au badge (permettant une identification du porteur lorsque la capture biométrique est inexploitable).

Les destinataires des informations seront, dans la limite de leurs attributions et pour la poursuite de la finalité précitée, les agents chargés de l'enregistrement des données sur le badge, les agents de sûreté visés à l'article L. 282-8 du code de l'aviation civile sur les points d'accès à la zone réservée, les administrateurs techniques et fonctionnels du traitement, et enfin les agents de l'Etat chargés du contrôle du personnel au sein de la zone réservée.

Néanmoins, l'historique des passages, le détail des accès empruntés ainsi que la liste des irrégularités seront uniquement accessibles aux administrateurs et personnels en charge de la maintenance des serveurs d'ADP.

Autorise, dans ces conditions, Aéroport de Paris à mettre en oeuvre le traitement de données à caractère personnel présenté.
Le président, Alex TURK.

Référence : CNIL, 08 mars 2007, *N° 2007-041 PORTANT AUTORISATION DE LA MISE EN OEUVRE PAR AÉROPORTS DE PARIS D'UN TRAITEMENT AUTOMATISÉ DE DONNÉES À CARACTÈRE PERSONNEL REPOSANT SUR LA RECONNAISSANCE DES EMPREINTES DIGITALES ET AYANT POUR FINALITÉ LE CONTRôLE DE L'ACCÈS AU SEIN...*, DROIT-TIC
http://www.droit-tic.com/juris/aff.php?id_juris=95

DROIT-TIC.com

R.D.T.I.C

LA REVUE DU DROIT DES TECHNIQUES DE L'INFORMATION ET DE LA COMMUNICATION-N°6 3 – AVRIL 2007

Dél. n° 2007-039 du 20 février 2007 portant refus d'autorisation de la mise en œuvre par la société Crown Worldwild SAS d'un traitement automatisé de données à caractère personnel ayant pour finalité la mise en place d'un dispositif d'alerte professionnelles

Thèmes
Informatique et libertés, droit social, droit du travail

Résumé
Délibération portant refus d'autorisation de la mise en oeuvre par la société Crown Worldwide SAS d'un traitement automatisé de données à caractère personnel ayant pour finalité la mise en place d'un dispositif d'alerte professionnelle.

Décision

COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTES - CNIL

Délibération 2007-039 du 20 février 2007

Délibération portant refus d'autorisation de la mise en oeuvre par la société Crown Worldwide SAS d'un traitement automatisé de données à caractère personnel ayant pour finalité la mise en place d'un dispositif d'alerte professionnelle.

La Commission nationale de l'informatique et des libertés ;
Vu la Convention n° 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;
Vu la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement de données à caractère personnel et à la libre circulation de ces données ;
Vu la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée par la loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, notamment son article 25-I-4° ;
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 demande d'autorisation, présentée par la société Crown Worldwide SAS d'un traitement automatisé de données à caractère personnel ayant pour finalité la mise en place d'un dispositif d'alerte professionnelle ;

Après avoir entendu M. Hubert BOUCHET, commissaire, en son rapport, et Mme Pascale COMPAGNIE, commissaire du Gouvernement en ses observations.

Formule les observations suivantes :

Le 12 septembre 2006, la société Crown Worldwide SAS a adressé à la Commission nationale de l'informatique et des libertés une déclaration relative à la mise en oeuvre d'un traitement de données à caractère personnel ayant pour finalité la mise en place d'un système externe et limité d'alertes éthiques visant à permettre à tout salarié s'estimant être témoin ou victime d'une situation de harcèlement sexuel ou moral ou d'une discrimination, de la signaler à un prestataire extérieur chargé par la société Crown de mener les investigations.

La Commission considère qu'il y a lieu de faire application des dispositions de l'article 25-I-4° de la loi du 6 janvier 1978 modifiée qui soumet à autorisation les traitements automatisés susceptibles, du fait de leur nature, de leur portée ou de leurs finalités, d'exclure des personnes du bénéfice d'un droit, d'une prestation ou d'un contrat en l'absence de toute disposition législative ou réglementaire.

Il convient d'examiner ledit traitement au regard des principes relatifs à la protection des données à caractère personnel, et notamment, de l'article 6-3° de la loi du 6 janvier 1978 modifiée qui dispose que les traitements ne peuvent 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.

La Commission considère que les dispositifs d'alerte professionnelle doivent être limités à un champ restreint aux domaines financier et comptable.

La Commission rappelle que, si elle admet que dans le cadre d'un dispositif d'alerte soient recueillis des faits graves ne relevant pas du strict domaine ne relevant pas des domaines financier et comptable lorsque l'intérêt vital de l'organisme concerné ou l'intégrité physique ou morale des employés est en jeu, elle estime que dans ces cas, le signalement de ces faits doit être réorienté vers les personnes compétentes au sein de l'entreprise concernée pour traiter ces faits, sans être exploité par les personnes gérant le dispositif d'alerte professionnelle. En outre, l'organisation chargée du traitement des alertes devrait détruire ou archiver sans délai les données relatives à cette alerte.

La Commission relève encore qu'aucun texte ne prévoit expressément les garanties et conditions susceptibles d'être mises en oeuvre par les employeurs qui envisageraient l'utilisation d'un dispositif externe d'alerte professionnelle dont le seul objet serait le signalement de situations de harcèlement ou de discrimination.

Compte tenu de l'ensemble de ces éléments et de la sensibilité d'un tel dispositif, le traitement n'apparaît pas, en l'état actuel des textes, proportionné à l'objectif poursuivi. En outre, le caractère adéquat, pertinent et non excessif des données collectées au regard des finalités ne peut être démontré à la Commission.

Dès lors, la Commission n'autorise pas, en l'état, la société Crown Worldwide SAS, sise 15 Avenue du Président Salvador Allende - 94400 Vitry Sur Seine, à mettre en oeuvre un traitement de données à caractère personnel ayant pour finalité la mise en place d'un dispositif d'alerte professionnelle.
Le président, Alex TURK.

Référence : CNIL, 20 février 2007, *2007-039 PORTANT REFUS D'AUTORISATION DE LA MISE EN OEUVRE PAR LA SOCIÉTÉ CROWN WORLDWIDE SAS D'UN TRAITEMENT AUTOMATISÉ DE DONNÉES À CARACTÈRE PERSONNEL AYANT POUR FINALITÉ LA MISE EN PLACE D'UN DISPOSITIF D'ALERTE PROFESSIONNELLE*, DROIT-TIC
http://www.droit-tic.com/juris/aff.php?id_juris=96

DROIT-TIC .com

R.D.T.I.C

LA REVUE DU DROIT DES TECHNIQUES DE L'INFORMATION ET DE LA COMMUNICATION-N°6 3 – AVRIL 2007

Dél. n° 2007-039 du 20 février 2007 portant refus d'autorisation de la mise en oeuvre par la société Kimberly-Clark SNC d'un traitement automatisé de données à caractère personnel ayant pour finalité la mise en place d'un dispositif d'alerte professionnelle

Thèmes
Informatique et libertés, droit social, droit du travail
Résumé
Dél. n° 2007-039 portant refus d'autorisation de la mise en oeuvre par la société Kimberly-Clark SNC d'un traitement automatisé de données à caractère personnel ayant pour finalité la mise en place d'un dispositif d'alerte professionnelle
Décision

COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTES - CNIL

Délibération 2007-040 du 20 février 2007

Délibération portant refus d'autorisation de la mise en oeuvre par la société Kimberly-Clark SNC d'un traitement automatisé de données à caractère personnel ayant pour finalité la mise en place d'un dispositif d'alerte professionnelle.

La Commission nationale de l'informatique et des libertés ;
Vu la Convention n° 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;
Vu la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement de données à caractère personnel et à la libre circulation de ces données ;
Vu la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée par la loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, notamment son article 25-I-4° ;
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 demande d'autorisation, présentée par la société Kimberly-Clark SNC d'un traitement automatisé de données à caractère personnel ayant pour finalité la mise en place d'un dispositif d'alerte professionnelle ;

Après avoir entendu M. Hubert BOUCHET, commissaire, en son rapport, et Mme Pascale COMPAGNIE, commissaire du Gouvernement en ses observations ;

Formule les observations suivantes :

Le 7 avril 2006, la société Kimberly-Clark SNC a adressé à la Commission nationale de l'informatique et des libertés une déclaration relative à la mise en oeuvre d'un traitement de données à caractère personnel ayant pour finalité la mise en place d'une ligne d'alerte professionnelle permettant aux salariés de "signaler à leur employeur des comportements qu'ils estiment contraires à l'éthique ou qui ne respectent pas la législation".

La Commission considère qu'il y a lieu de faire application des dispositions de l'article 25-14° de la loi du 6 janvier 1978 modifiée qui soumet à autorisation les traitements automatisés susceptibles, du fait de leur nature, de leur portée ou de leurs finalités, d'exclure des personnes du bénéfice d'un droit, d'une prestation ou d'un contrat en l'absence de toute disposition législative ou réglementaire.

Il convient d'examiner ledit traitement au regard des principes relatifs à la protection des données à caractère personnel, et notamment, de l'article 6-3° de la loi du 6 janvier 1978 modifiée qui dispose que les traitements ne peuvent 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.

La Commission considère que les dispositifs d'alerte professionnelle doivent être limités à un champ restreint aux domaines comptable, bancaire, financier et du contrôle des comptes.

La Commission estime en conséquence que les dispositifs d'alerte professionnelle doivent être conçus comme uniquement complémentaires par rapport aux autres modes d'alerte dans l'entreprise. Elle estime ainsi qu'afin de tenir compte de ce caractère intrinsèquement complémentaire, un dispositif d'alerte doit être limité dans son champ.

Or, en l'espèce, le dossier soumis à la CNIL par la société Kimberly-Clark SNC au soutien de sa demande d'autorisation indique clairement notamment d'une part que "le dispositif d'alerte n'a pas de champ d'application prédéterminé. Il peut concerner des sujets relatifs à la finance, la comptabilité, l'éthique". et fournit d'autre part une liste d'exemples de comportements pouvant être évoqués et traités par la ligne éthique tels que notamment : "(...) vol, usage ou vente de drogues illicites".

La Commission estime que l'absence de définition précise du champ du dispositif d'alerte soulève ainsi une difficulté de principe au regard de la loi, eu égard aux risques de mise en cause abusive ou disproportionnée de l'intégrité professionnelle voire personnelle des employés concernés.

Par ailleurs, la Commission considère que l'émetteur de l'alerte professionnelle doit s'identifier, son identité étant traitée de façon confidentielle par l'organisation chargée de la gestion des alertes. Elle estime encore que l'alerte d'une personne qui souhaite rester anonyme ne peut être recueillie que par exception et qu'à condition que le traitement des alertes anonymes soit entouré de précautions particulières, telles qu'un examen préalable, par son premier destinataire, de l'opportunité de sa diffusion dans le cadre du dispositif.

La Commission estime en outre que l'organisme mettant en place un dispositif d'alerte professionnelle n'incite pas les personnes ayant vocation à utiliser le dispositif à le faire de manière anonyme et que la publicité faite sur l'existence du dispositif en tienne compte, la procédure devant au contraire être conçue de façon à ce que les employés s'identifient auprès de l'organisation chargée de la gestion des alertes.

Or en l'espèce, l'utilisation anonyme du dispositif d'alerte présenté par la société KimberlyClark SNC apparaît clairement sinon comme la modalité privilégiée de signalement, au mieux comme une modalité pouvant être utilisée indifféremment à celle où l'émetteur de l'alerte est identifié.

En outre, le dossier demeure incomplet sur de nombreux points tels que, notamment: les modalités d'information des personnes concernées, la durée de conservation de données enregistrées, les mesures de sécurité, ainsi que les modalités d'exercice des droits d'accès et de rectification.

Au vu de l'ensemble de ces éléments, le traitement pris dans son ensemble n'apparaît, en l'état, ni adapté ni proportionné à l'objectif poursuivi. En outre, le caractère adéquat, pertinent et non excessif des données collectées au regard des finalités ne peut être démontré à la Commission.

Dès lors, la Commission n'autorise pas, en l'état, la société Kimberly-Clark SNC, sise 26 rue Armengaud - 92210 Saint-Cloud, à mettre en ceuvre un traitement de données à caractère personnel ayant pour finalité la mise en place d'un dispositif d'alerte professionnelle.
Le président, Alex TURK.

Référence : CNIL, 20 février 2007, *N° 2007-039 PORTANT REFUS D'AUTORISATION DE LA MISE EN OEUVRE PAR LA SOCIÉTÉ KIMBERLY-CLARK SNC D'UN TRAITEMENT AUTOMATISÉ DE DONNÉES À CARACTÈRE PERSONNEL AYANT POUR FINALITÉ LA MISE EN PLACE D'UN*