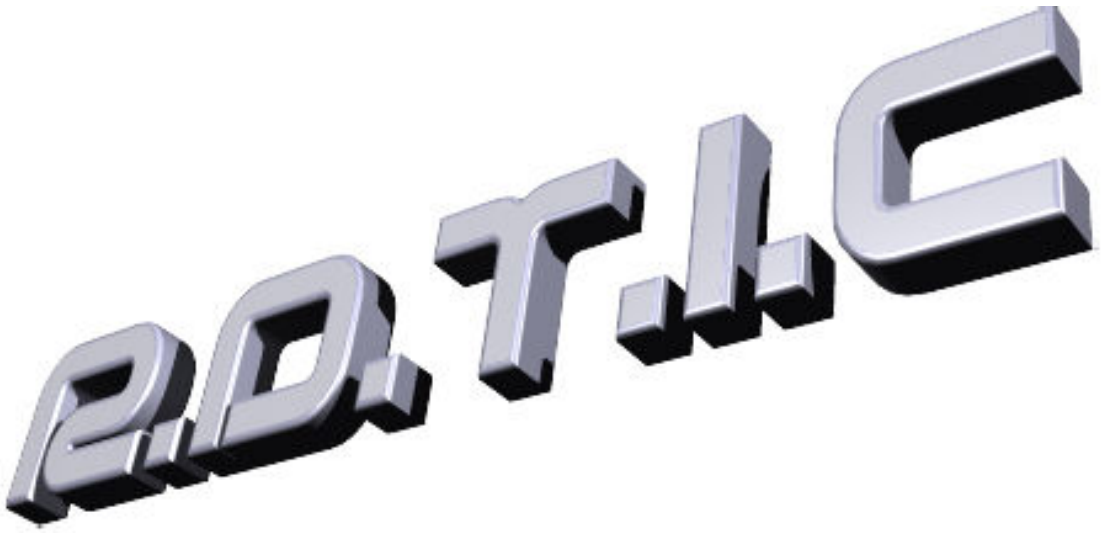
DROIT-TIC
REVUE DE DROIT DES TECHNIQUES DE L'INFORMATION ET DE LA COMMUNICATION
www.DROIT-TIC.com
N° 43 JUILLET 2005



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

N°43 - JUILLET 2005

www.DROIT-TIC.fr
Directeur de publication : Julien Le Clainche.
5 rue des chênes, 34110 Mireval.
Julien@droit-tic.com

ANALYSES

JURISPRUDENCE

DELIBERATIONS DE LA CNIL

Informatique et libertés, Droit pénal, Criminalité informatique

Vers une rétention des données relatives au trafic sans retenue ? - 18/07/2005

Par Julien Le Clainche, Allocataire de recherche .

Le Conseil extraordinaire Justice et Affaires Intérieures (JAI) a décidé le 13 juillet 2005 d'adopter la décision cadre sur la rétention de données au cours du Conseil JAI prévu le 12 octobre 2005 en dépit de son rejet par le parlement européen en juin 2004 et d'un avis défavorable du groupe de l'article 29

Les attentats survenus à Londres le 7 juillet 2005 mettent à nouveau sur le devant de la scène le projet de décision cadre[1] du Conseil européen relatif à la rétention des données de trafic[2]. Le Conseil extraordinaire Justice et Affaires Intérieures (JAI) a décidé le 13 juillet 2005 d'adopter la décision cadre sur la rétention de données au cours du Conseil JAI prévu le 12 octobre 2005 en dépit de son rejet par le parlement européen en juin 2004[3] et d'un avis défavorable du groupe de l'article 29[4].

Les questions de l'introduction des données de localisation[5] parmi les données relatives au trafic, et de la durée de conservation de l'ensemble de ces informations sont au centre des débats.

Les données relatives au trafic sont celles qui sont traitées en vue de l'acheminement d'une communication par un réseau de communications électroniques ou de sa facturation[6]. Les informations d'identification exigées par l'architecture des réseaux de communications constituent la base des données qui permettent la surveillance des transactions électroniques. Concrètement sur Internet, il peut s'agir des adresses « IP » auxquelles sont associées la date et l'heure de la connexion, le type d'usage, courriel, transfert de fichiers ou Web et des requêtes ou du message. Dans le cadre d'un réseau téléphonique, il pourra notamment s'agir des numéros appelants et appelés, de la date et de la durée de la communication, de l'identifiant du terminal. Il ne s'agit donc pas, en principe, de traiter le contenu des communications[7].

Le projet de décision cadre[8] propose d'y ajouter les données de localisation issues des réseaux de téléphonie mobile. C'est-à-dire toutes les données traitées dans un réseau de communications électroniques indiquant la position géographique de l'équipement terminal d'un utilisateur d'un service de communications électroniques accessible au public[9]. Il propose également une durée de conservation moyenne d'un an, qui pourra être étendue à trente-six mois dans les cas de terrorisme et de crime organisé.

Intérêts en présence

La protection des libertés individuelles et

publiques, dont notamment le droit des données personnelles, doit être mise en balance avec le besoin légitime de sécurité auquel peut s'attendre le citoyen. Il s'agit donc de trouver le point d'équilibre entre le nécessaire respect des principes inhérents à une société démocratique et les attentes de celle-ci en terme de sécurité.

Le développement des transactions électroniques a eu notamment pour conséquence de faciliter considérablement la circulation de l'information au niveau mondial. Ces nouveaux moyens de communication ont rapidement été mis à profit par les mouvances terroristes. Or, bien que l'Internet soit une technologie héritée de la culture militaire[10], les services de renseignements ont, semble-t-il, du mal à s'adapter à ce nouveau contexte. En effet, la transmission immédiate d'informations à moindre frais, par le biais d'un réseau de communication mondial pose de nombreux problèmes de régulation. Par exemple, comment retrouver les auteurs d'infractions, de délits ou de crimes sur le réseau, dans un monde ou chaque État à ses propres exigences souveraines, où chaque ordre juridique peut édicter des règles spécifiques à l'identification des personnes ?[11]. Afin de pouvoir réguler les comportements illicites sur Internet, il semble donc indispensable de conserver les informations permettant d'identifier les auteurs d'infractions, de délits ou de crimes. Toutefois, le fondement juridique et les garanties que doit apporter une société démocratique à ces traitements sont encore en question.

Un fondement juridique imparfait

L'article 15 de la directive 2002/58 CE précitée prévoit que pour sauvegarder la sécurité nationale - c'est-à-dire la sûreté de l'État - la défense et la sécurité publique, ou assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales ou d'utilisations non autorisées du système de communications électroniques, les États membres peuvent, entre autres, adopter des mesures législatives prévoyant la conservation de données pendant une durée limitée. L'article pose néanmoins la **condition que la « *limitation constitue une mesure nécessaire, appropriée et proportionnée, au sein d'une société démocratique* »**. Ainsi, les données identifiantes ne doivent pas être conservées au-delà de la période nécessaire à la réalisation de la finalité pour laquelle elles sont traitées. C'est donc la proportionnalité du traitement des données relatives au trafic qui est en question.

Toutefois, le rapporteur du parlement européen a mis en doute le fondement juridique de la décision cadre. En effet, celui-ci a distingué d'une part, « *la définition des données et leur durée de conservation, (..) qui relève du droit communautaire (…) [et] d'autre part, la proposition qui porte notamment sur l'accès et l'échange des données stockées dans les États membres, ce qui constitue une action commune dans le domaine de la coopération judiciaire en matière pénale et relève donc du troisième pilier* »[12]. Or, les obligations des fournisseurs de services sont déjà régies par des dispositions communautaires[13] au cours de l'élaboration desquelles, les États

membres ne sont pas parvenus à un accord sur la durée de conservation, ni sur la détermination des données concernées . De la sorte, la décision cadre serait susceptible d'affecter le traité instituant la communauté européenne, ce qui est interdit par l'article 47 du traité TUE.

Un dispositif inédit en droit français

La CNIL a souligné « *le caractère inédit du dispositif retenu* »[14], « *qui déroge au principe de finalité puisqu'il fait obligation aux opérateurs de communications électroniques de conserver, aux fins exclusives de faciliter le travail des autorités policières et judiciaires, des données qui se rapportent à l'ensemble des personnes utilisant leurs services et dont la conservation ne présente aucune utilité pour eux* »[15]. Si un opérateur ne conserve pas les informations relatives aux transactions électroniques de ses abonnés, il sera alors susceptible d'encourir une amende pouvant atteindre soixante-quinze mille euros sur le fondement de l'article L. 39-3 du code des postes et communication électroniques[16].

Un traitement qui doit constituer *« une mesure nécessaire, appropriée et proportionnée, au sein d'une société démocratique* ».

La conservation des données relatives au trafic sur une période trop longue entraîne des coûts élevés et des difficultés pratiques de traitement et notamment d'accès. Si toutes les données de trafic couvertes par la proposition devaient effectivement être conservées, le réseau d'un grand fournisseur d'accès Internet devrait stocker, en l'état actuel du trafic, un volume de données de vingt mille à quarante mille téraoctets. Or, une recherche dans une telle masse de d'information prendrait, en l'état de la technique, entre cinquante et cent ans[17]. En outre, il est fort probable que les auteurs de comportements illicites sauront passer inaperçus, puisque la sécurité informatique est loin d'être absolue et que l'usurpation d'identité est un fléau qui sévit sans relâche sur Internet[18].

Le coût de tels traitements peut représenter une charge importante pour l'industrie des télécommunications européenne. Dans le domaine de la téléphonie, le coût est estimé « *à 180 millions d'euros par entreprise, les coûts annuels d'exploitation pouvant atteindre les 50 millions d'euros (…) Les charges dans le domaine de l'Internet seraient plusieurs fois supérieures au montant des investissements nécessaires en matière de téléphonie filaire traditionnelle* »[19].

La nécessité et le caractère approprié de la mesure sont donc en question.

Ces considérations à la lumière du principe de proportionnalité ont conduit le rapporteur de la commission des libertés civiles du Parlement européen a conclure que le projet de décision cadre était «*inapproprié et déraisonnablement sévère*»[20].

Une atteinte à la présomption d'innocence ?

La conservation a priori d'informations identifiantes pose également la question de la présomption d'innocence dans une société démocratique. En effet, cette attitude prête à penser que chaque individu est un coupable potentiel, jusqu'à preuve de son innocence. Cette inversion de tendance est cependant une question plus sociétale, que juridique : Il s'agit de choisir vers quelle société nous voulons évoluer.

Par Julien Le Clainche, Allocataire de recherche .

1 Document du Conseil 8958/04 du 28 avril 2004. Conseil Européen,projet de décision cadre sur la conservation de données traitées et stockées en relation avec la mise à disposition de services de communications électroniques disponibles publiquement ou de données sur les réseaux de communications publiques aux fins de la prévention, l'étude, la détection et la poursuite des actes criminels, y compris le terrorisme, version partiellement publique du 8 novembre 2004.

2 Pour une chronologie complète des mesures relatives à la rétention des données de trafic, voir l'indispensable page de l'association**Imaginons un Réseau Internet Solidaire** (I.R.I.S),Rétention des données de trafic dans les communications électroniques, suivi des mesures françaises et européennes et de la plainte d'IRIS contre la France auprès de la CE (LSQ)

3 A. Nuno Alvaro, rapport 2004/0813(CNS) au Parlement européen pour la commission des libertés, de la justice et des affaires intérieures.

4 Groupe de l'article 29,Avis 9/2004 sur le projet de décision cadre sur la conservation de données traitées et stockées en relation avec la mise à disposition de services de communications électroniques disponibles publiquement ou de données sur les réseaux de communications publiques aux fins de la prévention, l'étude, la détection et la poursuite des actes criminels, y compris le terrorisme. [proposition présentée par la France, l'Irlande, la Suède et la Grande-Bretagne (Document du Conseil 8958/04 du 28 avril 2004), adopté le 9 novembre 2004.

5 Directive 2002/58 CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques, JOCE du 23 Novembre 1995 n° L. 281 p. 31. Article 2. c) : « *Toutes les données traitées dans un réseau de communications électroniques indiquant la position géographique de l'équipement terminal d'un utilisateur d'un service de communications électroniques accessible au public* ».

6 Code des postes et communications électroniques, article L.32 18°. Directive 2002/58 CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques, JOCE du 23 Novembre 1995 n° L. 281 p. 31. Article 2. b)

7 Loi n° 2000-719 du 1er août 2000 modifiant la loi n° 86-1067 du 30 septembre 1986 relative à la liberté de communication, J.O n° 177 du 2 août 2000 page 11903. Loi n° 91-646 du 10 juillet 1991 relative au secret des

correspondances émises par la voie des communications électroniques. Loi 2003-239 du 18 mars 2003 pour la sécurité intérieure, J.O n°66 mars 2003, p.4761

8 Document du Conseil 8958/04 du 28 avril 2004.

9 Directive 2002/58 CE du 12 juillet 2002, article 2. c).

10 A.SERRES, *Aux sources d'Internet : l'émergence d'ARPANET* , Thèse de Doctorat en Sciences de l'Information et de la Communication, Rennes II, 2000. 2 vol. Presses Universitaires du Septentrion (2003), coll. Thèse à la carte.

11 Les États-Unis ont historiquement un avantage sur les autres États puisque qu'ils sont à l'origine et contrôlent le système d'adressage sur Internet. Voir notamment, P. Crouzillacq,*Les Etats-Unis veulent conserver le contrôle d'Internet*, 01net, 6 juillet 2005.

12 A. Nuno Alvaro, rapport 2004/0813(CNS) au Parlement européen pour la commission des libertés, de la justice et des affaires intérieures, p. 6.

13 Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, JOCE du 23 Novembre 1995 n° L. 281, p. 31, article 1 et 2, a).

14 CNIL, délibération 01-018 du 03 mai 2001 portant avis sur le projet de loi sur la société de l'information, in CNIL, « 22ème rapport d'activité 2001 », Paris, La Documentation française, 2002,annexes, p.226.

15 Commission Nationale de l'Informatique et des Libertés, « Rapport d'activité 2003 », N°24, La Documentation française, 2004, p. 42.

16 Article L. 39-3 du code des postes et des communications électroniques : « *I. - Est puni d'un an d'emprisonnement et de 75000 euros d'amende le fait pour un opérateur de communications électroniques ou ses agents : (…) 2º De ne pas procéder à la conservation des données techniques dans les conditions où cette conservation est exigée par la loi.*».

17 Sur ce point voir, A. Nuno Alvaro, rapport 2004/0813(CNS) p. 7 : « *Given the volume of data to be retained, particularly Internet data, it is unlikely that an appropriate analysis of the data will be at all possible*.»

>« *If all the traffic data covered by the proposal did indeed have to be stored, the network of a large Internet provider would, even at today's traffic levels, accumulate a data volume of 20 - 40 000 terabytes. This is the equivalent of roughly four million kilometres' worth of full files, which, in turn, is equivalent to 10 stacks of files each reaching from Earth to the moon. With a data volume this huge, one search using existing technology, without additional investment, would take 50 to 100 years. The rapid availability of the data required seems, therefore, to be in doubt*».

18 « *Selon la FTC (Commission fédérale du commerce aux États-Unis), 10 millions d'Américains furent victimes d'usurpation d'identité numérique l'an passé, entraînant un coût pour les entreprises ou les particuliers estimé à 50 milliards de dollars* ».Proposition de loi tendant à la pénalisation de l'usurpation d'identité numérique sur les réseaux informatiques, Nº 452.

19 A. Nuno Alvaro, rapport 2004/0813(CNS), p. 8.

Informatique et libertés, Droit de la consommation, protection du consommateur

Vers une définition des espiogiciels - 16/07/2005

Par Julien Le Clainche, Allocataire de recherche .

Le terme « espiogiciel » ou « logiciel espion », issu de l'anglais « spyware » sert à décrire un programme, ou une partie de programme informatique, dont la fonction est de traiter, à l'insu de la personne concernée, les informations présentes sur le terminal de communication sur lequel il est implanté.

Le vocabulaire juridique de l'Internet a fait l'objet de nombreuses recherches de définition[1]. Toutefois, il ne prend pas encore en considération les « espiogiciels », mais seulement les « mouchards », qui sont assimilés aux témoins de connexion[2].

Les ordres juridiques anglo-saxons accordent une plus grande place aux définitions que les systèmes romano-germaniques. Il n'est donc pas surprenant que ce soit d'outre Atlantique que nous parvienne la première tentative de définition des « espiogiciels ». C'est donc tout un glossaire relatif aux techniques intrusives que vient de rendre public la « Anti-Spyware Coalition » (A.S.C). Ces définitions ne se sont pas encore réellement fixées puisqu'elles sont proposées aux internautes jusqu'au 12 août, afin que ceux-ci puissent les commenter.

L'«A.S.C » regourpe des éditeurs de logiciels "anti-spyware", des associations de consommateurs et des professionnels de la sécurité et de l'accès internet[3]. **L'objectif de la démarche est de dégager une unité terminologique, qui corresponde à la réalité pratique caractérisée par l'éclatement des techniques intrusives**. Il s'agit donc de déterminer les critères essentiels de qualification des « espiogiciels », afin de pouvoir définir des standards indispensables à la coordination de la lutte contre ces phénomènes intrusifs.

Le document soumis au public propose deux définitions des « espiogiciels ». D'une part, **il peut s'agir, dans une conception restrictive, d'un logiciel de surveillance implanté à l'insu de la personne concernée ou sur lequel elle n'a pas de contrôle** : « *Spyware is a term for Tracking Software deployed without adequate notice, consent, or control for the user*».

D'autre part, au sens large, il peut aussi s'agir de toute technique intrusive, « *In its broader sense, Spyware is used as a synonym for what the ASC calls "Spyware and Other Potentially Unwanted Technologies*." ». Seront alors concernés par la définition, non seulement les moyens logiciels, mais aussi les témoins de connexion ou les applets java.

Le document de travail de l'« A.S.C »

propose également des définitions concernant les « enregistreurs de frappe » (Keyloggers)[4], les connexions non sollicitées à des services de téléphonie (dialers)[5], ou encore le maintient en position ouverte des ports de connexion de l'ordinateur (backdoors)[6], les témoins de connexion[7], les témoins de connexion persistants[8], les Chevaux de Troie[9] les virus[10], les vers[11] ou encore les « adwares »[12]....[13]

En droit français, l'installation d'un logiciel-espion sur le terminal de communication à l'insu de son propriétaire constitue en principe un accès non autorisé à un système automatisé de données, qui est sanctionné par le chapitre III du code pénal intitulé : « *Des atteintes aux systèmes de traitement automatisé de données* ». L'utilisation de ce logiciel aux fins transmettre les données personnelles de la personne concernée à son insu constitue également un délit pénal, dont la sanction sera aggravée dans l'hypothèse d'une transmission vers un pays tiers à la communauté européenne. Les sanctions sont édictées aux articles 226.-16 à 226-24 du Code pénal.

Toutefois, organiser le respect des dispositions pénales de droit français n'est pas toujours aisé. En effet, **le principe de territorialité applicable aux lois de polices n'est pas toujours évident à concilier avec la souveraineté des États. C'est pourquoi l'établissement de standards commun à l'ensemble des ordres juridiques est un préalable nécessaire à la régulation des comportements illicites sur l'Internet. Pourtant, l'unification recherchée par la « A.S.C » est réalisée essentiellement sous l'influence des acteurs du marché et constitue donc une démarche d'auto régulation, par nature limitée.**

*** Pour faire part de vos opinions à l' « A.S.C » quant à ces propositions de définitions, cliquez ici.**
*** Pour plus d'information sur les logiciels indiscrets consultez sur DROIT-TIC : B. EGRET, *LES PROBLÈMES JURIDIQUES DES LOGICIELS INDISCRETS*, mémoire de DEA, ERID, 2003** ;

Par Julien Le Clainche, Allocataire de recherche .

1 Voir par exemple, « Vocabulaire de l'informatique et de l'internet : liste des termes, expressions et définitions adoptés » J.O du 16 mars 1999, p. 3905-3910.Voir aussi, Commission générale de terminologie et de néologie, Vocabulaire de l'informatique (liste de termes, expressions et définitions adoptés), J.O n° 49 du 27 février 2003 page 3531 J.O n° 49 du 27 février 2003 page 3531

2 Appliquette envoyée par un serveur de la toile mondiale à un utilisateur, parfois à l'insu de celui-ci, au cours d'une connexion, afin de caractériser cet utilisateur. 2. Par extension, information que l'appliquette peut enregistrer sur le disque de l'utilisateur et à laquelle le serveur peut accéder ultérieurement. J.O du 16 mars 1999, p. 3910.

3 Les participants sont : * Aluria * AOL * Computer Associates * Dell, Inc. * EarthLink * F-Secure Corporation * HP * Lavasoft * McAfee Inc. * Microsoft * Panda Software * PC Tools * Safer-Networking Ltd. * Symantec * Tenebril * Trend Micro * Webroot Software * Yahoo! Inc. * Center for Democracy & Technology * Samuelson Law,

Technology & Public Policy Clinic at Boalt Hall, UC Berkeley School of Law * The Canadian Internet Policy and Public Interest Clinic The Cyber Security Industry Alliance. Coordination : The Center for Democracy and Technology convened the Anti-Spyware Coalition.. Source : http://www.antispywarecoalition.org/about/index.htm.

4 **Keylogger (or Keystroke Logger):** *Tracking Software* that surreptitiously records keyboard and/or mouse activity. Keyloggers typically either store the recorded keystrokes for later retrieval or they transmit them to the remote process or person employing the Keylogger.

5 **Dialer**: A program that utilizes a computers modem to make calls or access services. Users may want to remove dialers that can result in unexpected phone numbers being dialed or unexpected telephone charges. Dialer is a colloquial term for *Dialing Software*.

6 **Backdoor:** A type of *Remote Control Software* that enables a third party to covertly control system resources.

7 **Cookie :** *A piece of data that a web site, through the means of the browser, saves on users computers hard drives and retrieves when they revisit that Web site or an affiliated site. Some cookies may use a unique identifier that links to information such as login or registration data, online shopping card selections, user preferences, web sites you have visited, etc...*

8 **Tracking Cookies:** A Tracking Cookie is any cookie used for tracking users' surfing habits. TrackingCookies are a form of *Tracking Technology*. They are typically used by advertisers wishing to analyze and manage advertising data, but they may be used to profile and track user activity more closely. However, tracking cookies are far more limited in their ability to track users than software that is actually installed on users computers. While installed software can potentially record any data or activity on a computer (*see* System Monitor), cookies can only record visits or activity on a single website or its affiliated sites. Moreover, unlike Tracking Software, cookies entail no substantial effect on computer reliability, security, or speed.

9 **Trojan**: A non-replicating malicious program designed to appear harmless or even useful to the user, but, when executed, harms the user's system. Some software bundles containing malicious forms of spyware or other potentially unwanted software are considered to be Trojans.

10 **Virus**: Self-replicating code that propagates by reproducing and inserting itself into other programs, documents, or email attachments. Some viruses are intentionally destructive (for example, erasing information on users' hard drives). For others, the primary negative effect is their uncontrolled selfreproduction, which can overwhelm system resources.

11 **Worm:** A computer worm is a self-replicating computer program, similar to a computer virus. Unlike viruses, however, worms self-propagate and so do not require other programs or documents to spread. Worms typically spread through email or other file transmission capabilities found on networked computers.

12 **Adware:** A type of *Advertising Display Software*, specifically certain executable applications whose primary purpose is to deliver advertising content in a manner or context that potentially may be unexpected and unwanted by users. Many Adware applications also perform tracking functions, and therefore may also be categorized as *Tracking Technologies*. Consumers may want to remove Adware if they object to such tracking, do not wish to see the advertising caused by the program, or are frustrated by its effects on system performance. Some users may wish to keep particular Adware programs if their presence subsidizes the cost of a desired product or service or if they provide advertising that is useful or desired.

13 Pour une liste complète, consultez le glossaire de « l'anti-Spyware Coalition ».

Propriétés intellectuelles, Responsabilité

Le Peer to Peer fusillé par la Cour Suprême des Etats-Unis : lorsque la Haute Cour américaine redéfinit la légalité des moyens de copie - 11/07/2005

Par M. Sulliman Omarjee, Juriste .

Jusqu'à présent et en vertu de la jurisprudence SONY BETAMAX de 1984, les fabriquants ne pouvaient être tenus pour responsables de l'utilisation faite de ces appareils par les consommateurs même si cette utilisation violait la loi sur le copyright, dès lors qu'ils ne démontraient aucun pouvoir de contrôle sur cette utilisation.

Etonnant renversement de situation : la Cour Suprême des USA, appelée à se prononcer sur la légalité des logiciels peer to peer Grokster et Morpheus, a durci sa position s'agissant de la légalité des appareils de copie !

Jusqu'à présent et en vertu de la jurisprudence SONY BETAMAX de 1984[1], les fabriquants ne pouvaient être tenus pour responsables de l'utilisation faite de ces appareils par les consommateurs même si cette utilisation violait la loi sur le copyright, dès lors qu'ils ne démontraient aucun pouvoir de contrôle sur cette utilisation. En d' autres termes, lorsqu' un appareil est susceptible à la fois d' un usage licite et illicite au regard de la loi sur le copyright (un appareil « mixte »), la responsabilité de son fabriquant ne peut être engagée. Il en irait différemment si l' usage permis par l' appareil est exclusivement illicite.

Cette décision fort juste privilégiait la protection de la recherche et de l' innovation. Une solution contraire aurait en effet abouti à freiner le progrès technique sur le fondement de la nécessaire protection du copyright

C' est ainsi que, grâce à la jurisprudence SONY, plusieurs technologies de copie ont pu voir le jour en toute licéité : graveur, encodage, numérisation… A maintes reprises, la jurisprudence SONY avait été invoquée avec succès lors de litiges mettant en cause les fabricants de ces nouvelles techniques : le lecteur mp3 RIO par exemple, mais également les logiciels peer to peer Kazaa et Grokster. Elle avait même inspiré une décision similaire en Grande Bretagne s' agissant du radio double cassette[2] ou encore aux Pays-Bas s' agissant du logiciel Kazaa[3].

L' un des rares cas ou elle n'avait pas été retenue était celui du célèbre Napster : du fait de l'existence d'un serveur central, la Cour de New York avait considéré que la société Napster avait un pouvoir de contrôle sur l'utilisation faite par les consommateurs du logiciel du même nom[4]. Similairement, la compagnie Aimster s' était vu condamnée pour les infractions au copyright rendue possibles via son service qu' elle « *encourageait, dirigeait et dont elle bénéficiait financièrement* »[5].

Désormais, il semblerait que le bénéfice de l'exception SONY BETAMAX soit

encadré de manière beaucoup plus stricte. En effet, pour condamner les compagnies GROKSTER et Morpheus sur le fondement de la violation de copyright, la Cour suprême, considère maintenant que :

«*Quiconque distribue un appareil dans l'objectif de promouvoir son utilisation à des fins de violation de copyright, que ce soit par le biais de messages clairs ou d'autres actes encourageants à l'évidence l'infraction, est responsable de ces actes de violation*»[6]

Surprenante, cette décision pourrait dans un premier temps être perçue comme la fin de la jurisprudence SONY, la mort (juridique du moins) des systèmes peer to peer, un coup d' arrêt au progrès technique : va-t-on demain poursuivre les fabriquant de graveurs de dvd, de logiciels de compression de fichiers et autres technologies similaires permettant la reproduction d'oeuvres protégées au risque d' entraver la liberté d' innover ?

Une lecture plus attentive de la décision permet cependant de relativiser sa portée.

En effet, ce que la Haute Cour condamne ici, ce n' est pas la fabrication ni même la simple distribution d' un appareil ou d' une technologie dite « mixte », mais **la promotion de l' usage illicite** qu' on peut en faire. Pour que cette notion de promotion illicite puisse être retenue, la Cour exige que soit caractérisé :

- une intention claire de porter atteinte au copyright (*clear expression*), pouvant être caractérisée par des actes positifs de promotion (*active steps*) ;

- la conscience que les tiers utilisateurs dudit appareil vont grâce à la promotion faite, se livrer à des actes enfreignants le copyright (*with knowledge of third parties action*) ;

En l' espèce, la Cour considère que l' intention claire de porter atteinte au copyright est démontrée dès lors que :

- Morpheus et Grokster ont été présentés comme des alternatives au feu Napster avec une intention manifeste de capter ses utilisateurs éconduits

- les sociétés exploitant ces logiciels n' ont fait aucun effort pour limiter les activités contrefaisantes

- elles se sont enrichies par la publicité vendue sur leurs espaces lors de l' utilisation de leurs services

La décision ne remet pas en cause la jurisprudence SONY. En revanche, elle rend plus difficile son bénéfice, les juges considérant qu' elle n' exonère pas un fabricant de sa responsabilité du seul fait que le produit qu' il a créé est susceptible d' un usage mixte[7].

Faut-il déduire de cet arrêt l' illégalité de tous les systèmes peer to peer ? Cela serait quelque peu hâtif, les juges ayant apparemment voulu circonscrire leur solution aux faits particuliers qui leur étaient soumis, visiblement dans le but de préserver la continuité de la jurisprudence SONY au service de l' innovation[8]. Il n' empêche que par cette décision, elle ajoute un degré de responsabilité supplémentaire pour les

fabricants qui doivent désormais s' interdire de tout acte positif de promotion d' un usage illicite de leurs produits. En clair, **il n' est pas interdit de créer des produits mixtes, ce qui est interdit c' est d' en vanter les utilisations violant le copyright**.

De là à dire que le peer to peer est condamné…

Par Sulliman OMARJEE
Juriste de Propriété Intellectuelle et NTIC à la Région Réunion
DEA de Droit des Créations Immatérielles - LLB- WIPO
s.omarjee@laposte.net
http://sullimano.tooblog.fr/

Par M. Sulliman Omarjee, Juriste .

1 SONY vs Universal City Studios 104 US 774 (1984).

2 CBS Songs vs Amstrad (1988) RPC 567.

3 « *Kazaa could not prevent the exchange of copyright material by suscribers so the service itself was not unlawful even if the activities of suscribers were illegal* ».

4 RIAA vs NAPSTER (2000) 9th US Circuit Court of Appeal.

5 « *Aimster showed wilful blindness to copyright infringement and could have limited infringement … It was for Aimster to show that its service had non infringing uses* » Federal Court of Appeal 2003, Aimster.

6 « *We hold that one who distributes a device with the object of promoting its use to infringe copyright, as shown by clear expression or other affirmative steps taken to foster infringement, is liable for the resulting acts of infringement by third parties.* »

7 « *Nothing in Sony requires courts to ignore evidence of intent to promote infringement if such evidence exists. It was never meant to foreclose rules of fault-based liability derived from the common law (464 U. S., at 439). Where evidence goes beyond a product.s characteristics or the knowledge that it may be put to infringing uses, and shows statements or actions directed to promoting infringement, Sony' s staple-article rule will not preclude liability. At common law a copyright or patent defendant who not only expected but invoked [infringing use] by advertisement was liable for infringement.* » Voir également Etienne Wery, "La cour suprême américaine signe l' arrêt de mort de deux réseaux peer-to-peer", http://www.droit-technologie.org , 29 Juin 2005,

8 « *The tension between the competing values of supporting creativity through copyright protection and promoting technological innovation by limiting infringement liability is the subject of this case.* »

Informatique et libertés, droit social, droit du travail

La cour de cassation précise les conditions d'accès aux fichiers informatiques personnels des salariés -01/07/2005

Par Me. Martine Ricouart-Maillet, Avocate associée, cabinet BRM. et M. Nicolas Samarcq Juriste BRM AVOCATS.

Philippe K. a été licencié pour faute grave à la suite de la découverte de photos érotiques dans un tiroir de son bureau, il avait été procédé à une recherche sur le disque dur de son ordinateur qui avait permis de trouver un ensemble de dossier...

L'arrêt « Nikon » du 2 octobre 2001 (pdf) avait reconnu au salarié le droit au respect de l'intimité de sa vie privée sur leur lieu de travail. Cela implique « *que l'employeur ne peut dès lors sans violation de cette liberté fondamentale prendre connaissance des messages personnels émis par le salarié et reçus par lui grâce à un outil informatique mis à sa disposition pour son travail et ceci même au cas où l'employeur aurait interdit une utilisation non professionnelle de l'ordinateur* ».

La Cour de cassation, dans un arrêt du 17 mai 2005[1], a précisé les conditions dans lesquelles l'employeur peut accéder aux fichiers personnels d'un salarié enregistrés sur le disque dur de son poste de travail : « *Attendu que, sauf risque ou événement particulier, l'employeur ne peut ouvrir les fichiers identifiés par le salarié comme personnels contenus sur le disque dur de l'ordinateur mis à sa disposition qu'en présence de ce dernier ou celui-ci dûment appelé ; Qu'en statuant comme elle l'a fait, alors que l'ouverture des fichiers personnels, effectuée hors la présence de l'intéressé, n'était justifiée par aucun risque ou événement particulier, la cour d'appel a violé (...)* », l'article 8 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, l'article 9 du Code civil, l'article 9 du nouveau Code de procédure civile et l'article L.120-2 du code du travail.

Cet arrêt étend au domaine informatique la solution dégagée par la Cour de cassation dans un arrêt du 11 décembre 2001 relatif aux conditions de contrôle du contenu d'une armoire d'un employé. En l'espèce, la Cour avait précisé que le règlement intérieur doit prévoir l'éventualité d'un tel accès ainsi qu'une information préalable du salarié (qui doit être présent au moment de la vérification du contenu ou au moins être prévenu). Exceptionnellement, le contrôle de cette espace réservé est possible sans inscription au règlement intérieur et sans information préalable du salarié en cas de « *risque ou d'événement particulier* ». En l'espèce, la Cour avait considéré que la fouille de l'armoire individuelle ayant permis la découverte de boissons alcoolisées n'était justifiée par aucun risque ou événement particulier.

Reste à la jurisprudence à définir ce qu'elle entend par « *risque ou*

événement particulier », ce qui vraisemblablement sera fait au cas par cas.

Par Me. Martine Ricouart-Maillet, Avocate associée, cabinet BRM. et M. Nicolas Samarcq Juriste BRM AVOCATS.

1Cour de cassation, Chambre sociale, 17 mai 2005, Philippe K. / Cathnet-Science disponible sur **www.droit-tic.fr.**

Tribunal de grande instance de Paris, ordonnance de référé du 08 juillet 2005, PMU C/ ETURF, ZETURF

Thèmes
Contenus et comportements illicites, Loi applicable et juridiction compétente

Abstract
Contenus et comportements illicite - courses hippiques - prise de pari - autorisations délivrées par le ministère de l'agriculture (absence) - fermeture du site (oui)

Résumé
Une société de prise de pari en ligne dans le domaine des courses hippiques porte atteinte à la loi du 2 juin 1891.

Décision

Vu l'assignation délivrée le 27 juin 2005 par le Groupement d'intérêt économique Pari Mutuel Urbain (PMU), suivant laquelle il est demandé en référé de :

Vu l'article 809 du ncpc, l'article 4 de la loi du 2 juin 1891 modifiée par la loi du 10 mars 2004,
. ordonner aux sociétés Eturf et Zeturf Ltd, sous astreinte de 50 000 € par jour de retard à compter de la décision à intervenir, de cesser l'édition sur internet et aux adresses zeturf.com et zeturf.fr ou à toutes autres adresses internet, de toutes activités de prise de paris en ligne sur les courses hippiques organisées en France,
. la condamner au paiement de la somme de 10 000 € en application de l'article 700 du ncpc et au paiement des dépens de la présente instance.

Vu les conclusions de la société Eturf, qui demande qu'il lui soit donné acte de ce qu'elle ne participe en aucune façon à une activité de prise de paris en ligne sur les courses hippiques organisées en France, et de débouter le PMU de l'intégralité de ses

demandes ;

Vu les conclusions en réplique du PMU ;

Attendu que la société de droit maltais Zeturf ne comparait pas, ni n'est représentée à l'audience ;

Qu'en application des dispositions de l'article 472 du ncpc il ne sera fait droit aux demandes dirigées contre elle que pour autant qu'elles apparaissent régulières, recevables et bien fondées ;

Sur la procédure :

Attendu que l'acte introductif destiné à la société Zeturf Ltd a été adressé le 27 juin 2005 à l'entité requise à Malte, conformément aux dispositions du règlement du conseil de l'union européenne n°1348/2000 du 29 mai 2000, ce dont celle-ci a accusé réception le 1er juillet 2005 ;

Qu'il est également justifié de la traduction de l'acte en langue anglaise ;

Qu'en cours de délibéré le demandeur a transmis avec notre accord des pièces justifiant de la signification de l'acte introductif, faisant apparaître que celle-ci a été effectuée le 4 juillet 2005, jour de l'audience, en deux adresses différentes, respectivement à 13h45 et 13h57, conformément par conséquent aux dispositions de l'article 7 du règlement en question ;

Que la procédure est par conséquent régulière ;

Qu'en outre il est justifié de la délivrance de l'acte le 4 juillet 2005, à 13h45, au domicile parisien de M. Emmanuel de RC dirigeant de la société Zeturf Ltd, à la personne de son employée de maison qui a accepté de recevoir l'acte, l'affaire ayant été appelée à l'audience tenue le même jour à 16 h ;

Qu'il s'agit dès lors d'apprécier si l'urgence est de nature à justifier en l'espèce l'examen des mesures provisoires demandées, au sens des dispositions de l'article 19.2 du règlement ;

Le PMU expose qu'en application des dispositions de la loi du 2 juin 1891, modifiée par l'article 186 de la loi de finances du 16 avril 1930 et du décret du 5 mai 1997 (modifié par le décret du 12 novembre 2002), les sociétés de courses sont autorisées à organiser des courses hippiques sur leurs hippodromes et à recueillir sur celles-ci des paris collectés sur et en dehors des hippodromes, et que le PMU, groupement qui regroupe actuellement 71 sociétés de courses, est seul habilité à collecter les paris en dehors des hippodromes.

Il évoque un premier litige survenu avec la société Zeturf.com devenue Eturf, constituée en octobre 2000, et qui exploitait jusqu'alors un site internet consacré uniquement à l'information sur les courses hippiques, accessible par les adresses www.zeturf.com et www.zeturf.fr.

Ayant constaté des extractions à son sens substantielles et des réutilisations anormales de sa base de données par ce site, il faisait dans un premier temps constater ces extractions par huissier de justice le 19 octobre 2004, en glissant volontairement une erreur sur les cotes publiées sur le site www.pmu.fr, immédiatement reprise sur le site litigieux zeturf.com dont l'éditeur est la société du même nom.

Il procédait ensuite le 3 février 2005 à une saisie contrefaçon au cours de laquelle les personnels de Zeturf.com auraient reconnu

le caractère illicite de l'extraction, suivie de l'introduction d'une instance actuellement pendante devant le tribunal de grande instance de Paris, 3ème chambre.

Le demandeur précise que le 2 mai 2005, Emmanuel de RC, président du conseil d'administration de la société Zeturf.com démissionnait, pour être remplacé par Guillaume R. ; alors que cette société prenait une nouvelle dénomination, soit Eturf, la société de droit maltais Zeturf Ltd apparaissait le 19 juin 2005, animée par l'ancien dirigeant de Zeturf.com, pour lancer la prise de paris en ligne sur les courses françaises de chevaux.

Il expose ensuite que le 20 juin 2005, de nombreux organes de la presse française annonçaient que le site litigieux offrait désormais la prise de paris en ligne sur les courses hippiques françaises, et non plus seulement des informations ; Emmanuel de RC, fondateur, communiquait à ce sujet pour annoncer des rapports supérieurs à ceux du PMU, expliquant que le site litigieux était désormais exploité par cette société de droit maltais, autorisée par l'autorité publique maltaise à exercer l'activité contestée.

Le demandeur, soutenant que Emmanuel de RC reste le véritable animateur de la société Eturf, fait état d'un trouble à caractère manifestement illicite qu'il s'agirait de faire cesser, dans la mesure où cette activité est exercée en fraude à la loi, et porte atteinte à l'ordre public, au budget de l'Etat français et à la filière hippique française ; il cite les dispositions de l'article 4 de la loi du 2 juin 1891 modifiée par la loi du 10 mars 2004.

Il en veut pour preuve l'identité entre le site exploité et celui édité à la même adresse par la société de droit français Eturf, anciennement Zeturf.com, tel que le faisait apparaître le constat dressé le 19 octobre 2004, maintenant consacré non plus à la fourniture d'information sur les courses de chevaux, mais à l'organisation de paris sur des courses de chevaux organisées en France, son édition exclusivement en langue française le destinant dès lors manifestement à un public de langue française, échangeant par courriers électroniques en langue française, comme constaté le 21 juin 2005.

Il observe encore dans l'acte introductif que l'adresse internet zetruf.fr, propriété de la société Eturf anciennement Zeturf.com figure toujours et donne accès au site, d'ailleurs hébergé par une société française située à Toulouse, de sorte qu'il y aurait co-édition des sites litigieux par les sociétés Eturf et Zeturf Ltd.

Il ajoute que les sociétés de courses ont pour vocation l'amélioration de la race chevaline en France, obtenue par l'organisation de courses hippiques qui permettent, grâce aux prélèvements sur les paris mutuels et après déduction des frais de gestion du PMU et de ce qui revient à l'Etat, d'assurer le financement de toute la filière hippique sous la tutelle du ministère de l'agriculture, du ministère de l'économie, des finances et de l'industrie, et du ministère de l'intérieur.

Ainsi serait porté atteinte à ses yeux à l'intérêt général, dans la mesure où l'ensemble de la filière hippique, de l'élevage aux métiers des équipements et des matériels liés aux activités hippiques, représenterait en France 59 000 emplois directs et 130 000 emplois indirects, ainsi qu'aux intérêts de l'Etat français, régulateur de l'offre de paris en France, privé du fait de cette activité des recettes tirées des prélèvements opérés sur les paris.

Il caractérise l'urgence par l'ampleur des intérêts en jeu, la prise de paris en ligne étant actuellement active.

La société Eturf explique qu'elle a décidé fin 2004 de consacrer son activité exclusivement à la fourniture de contenu à la presse spécialisée, et de céder l'exploitation du site internet "zeturf.com", en voulant pour preuve la signature d'un contrat le 8 février 2005 avec une société RBP Ventures Ltd, la modification de sa dénomination sociale, et la mention de la cession du nom de domaine le 14 février suivant.

Elle se déclare par conséquent étrangère à l'activité de prise de paris en ligne, et explique que ce n'est qu'à réception de l'acte introductif qu'elle a appris que les registres de l'Afnic n'avaient pas été mis à jour, seules les sociétés françaises ou inscrites à un registre national pouvant détenir un nom de domaine en .fr, ajoutant qu'elle a appris que ce nom de domaine "zeturf.fr" avait été détruit.

Le PMU répond que le contrat de cession, qui aurait dû emprunter la forme d'une cession de fonds de commerce, ne lui est pas opposable, que les mentions prescrites par l'article 6 III.1 de la loi 04-575 du 21 juin 2004 relatives aux coordonnées de l'éditeur et du prestataire d'hébergement font défaut sur le site, de sorte que tout transfert par la société Eturf à un tiers de l'exploitation de ce site lui serait également inopposable.

Sur l'application de l'article 19 du règlement :

Attendu que le demandeur, qui s'appuie sur les dispositions de l'article 809 du ncpc, justifie l'urgence à prendre des mesures par l'importance des intérêts en jeu, les faits allégués portant atteinte à la filière hippique française, financée via les sociétés de courses par l'activité du PMU, et qui représente plusieurs milliers d'emplois directs ou indirects ;

Qu'il résulte du constat dressé dès le 21 juin 2005, soit le lendemain de l'annonce publique par l'animateur déclaré du site litigieux du lancement de paris en ligne, que l'activité en question est effective ;

Que le demandeur rappelle qu'en vertu des dispositions de l'article 4 de la loi du 2 juin 1891 modifiée notamment par la loi 04-204 du 9 mars 2004, le fait d'offrir de ou de recevoir en quelque lieu et sous quelque forme que ce soit des paris sur les courses de chevaux expose son auteur à des sanctions pénales, alors que suivant l'article 5 les sociétés qui organisent des courses de chevaux ayant pour but exclusif l'amélioration de la race chevaline et dont les statuts ont été approuvés par le ministère de l'agriculture peuvent organiser le pari mutuel, moyennant autorisation spéciale du ministre de l'agriculture ;

Que c'est dans ces conditions que sa gestion a été confiée à un groupement d'intérêt économique constitué entre ces sociétés de courses, le PMU ainsi que précisé par le décret du 5 mai 1997, modifié par le décret 02-1346 du 12 novembre 2002 ;

Que dès lors qu'il est invoqué que l'activité qui résulte de l'offre proposée en ligne ne satisferait pas aux conditions strictement prévues par ces textes, dans l'intérêt en particulier du financement de la filière hippique française, il apparaît urgent d'examiner si la demande tendant à prendre les mesures demandées apparaît fondée ;

Qu'enfin, il doit être considéré dans le cadre de cette procédure ainsi justifiée par l'urgence que la société Zeturf Ltd a bénéficié d'un délai suffisant pour comparaître et préparer sa défense ; qu'en particulier, son dirigeant, à la suite du lancement public de l'activité litigieuse, ne pouvait que s'attendre à une réaction du demandeur, dans le contexte de

l'introduction antérieurement d'une autre instance relative aux conditions d'exploitation du même site internet qu'il ne pouvait ignorer ;

Sur les demandes :

A l'encontre de la société Zeturf Ltd

Attendu qu'il ressort du constat dressé le 21 juin 2005 le fait que le site se trouve exclusivement rédigé en langue française, et ne permet de prendre de paris qu'en cette langue, alors que les courses concernées se déroulent sur le territoire français ; que c'est l'internaute français qui est d'évidence visé ;

Qu'au demeurant, bien que le "règlement" affiché évoque la loi maltaise, l'accès au jeu se trouve interdit aux résidents maltais ;

Que dès lors, le lieu de réalisation du trouble, soit du fait dommageable au sens des dispositions de l'article 46 du ncpc, se situe bien en France, le constat ayant été dressé à Paris ;

Que c'est au PMU qu'a été confiée la gestion relative à l'organisation par les sociétés de courses autorisées du pari mutuel en dehors des hippodromes, comme prévu par l'article 27 du décret n°97-456 du 5 mai 1997 modifié par le décret n°02-1346 du 12 novembre 2002 ;

Que la prise de paris en ligne cause donc bien un trouble manifestement illicite au PMU, dès lors qu'elle n'a pas été autorisée ;

Attendu en revanche que le site fait apparaître au titre de "contact" la société Zeturf Ltd, avec son adresse et un numéro de téléphone à laquelle elle est peut être jointe, alors que les conditions générales consultables lors de l'inscription font apparaître l'adresse de son siège et le numéro de son immatriculation, outre un numéro de télécopie et une adresse électronique ;

Qu'au contraire le nom des prestataires d'hébergement n'apparaît pas affiché sur le site comme l'impose la loi, étant observé que le constat a néanmoins permis d'identifier l'un d'eux comme situé sur le territoire français, et le second sur le territoire allemand ;

Attendu qu'il peut encore être relevé au sujet du caractère illicite de cette activité de communication au public en ligne, que l'éditeur, tout en avertissant les seuls internautes résidents maltais et des Etats-Unis d'Amérique qu'ils ne peuvent s'inscrire, a cru bon de mentionner que les titulaires de compte sont invités à se plier à la législation en vigueur sur leur lieu de domicile et/ou de résidence, et que la participation à des paris pouvant être soumise à des restrictions légales et même être interdite dans certains pays, "ces restrictions ou interdictions peuvent être d'application, même si Zeturf Ltd dispose des licences indispensables à l'organisation et la prise de paris".

Attendu en définitive que les demandes tendant à faire injonction à la société Zeturf Ltd de cesser l'activité de prise de paris en ligne sur les courses hippiques organisées en France se fondent bien sur un trouble manifestement illicite ;

Qu'il convient d'y mettre fin ;

A l'égard de la société Eturf

Attendu que dès le 3 février 2005 le PMU diligentait une saisie contrefaçon dans les locaux de la société Zeturf.com, puis l'assignait le 16 devant ce tribunal ;

Que le 8 février suivant intervenait un contrat aux termes duquel les noms de domaine "zetruf.com" et "zeturf.fr" comme la marque "zeturf" étaient cédés à la

société RBP Ventures Ltd qui dans le même temps, suivant les écritures de la société Eturf, proposait au président du conseil d'administration de la société cédante de collaborer à son activité ; que de fait, Emmanuel de RC se présente lors d'entretiens récemment accordés à la presse comme étant directeur ou "managing director" de Zeturf Ltd ;

Que ce contrat, signé à Malte, et qui n'apparaît pas avoir été dénoncé à ce jour, accordait une licence d'utilisation non exclusive de l'ensemble des données relatives aux courses hippiques stockées dans la base de données liée à l'application avec les contrats de vente d'espace publicitaire ; qu'en outre, il était convenu entre la société Zeturf.com et la société de droit maltais cessionnaire la fourniture du contenu permettant à cette dernière de "continuer à procurer aux utilisateurs la même qualité d'information" ; que les pièces communiquées ne renseignent pas sur les liens contractuels directs éventuels entre la cédante et la société Zeturf Ltd ;

Que le nom de domaine "zeturf.com" apparaissait enregistré au nom de "Zeturf Ltd" au 14 février 2005, entité également situé à Malte, à une autre adresse toutefois que la RBP Ventures Ltd ; que de même, la société Zeturf.com changeait sa dénomination pour celle d'Eturf, comme cela ressort d'un extrait Kbis au 9 juin 2005, date à laquelle était enregistré le procès verbal de réunion du conseil d'administration portant la date du 2 mai précédent et constatant la démission de son président Emmanuel de RC ;

Qu'il peut de même être relevé que l'inscription au registre national de la marque au nom de "Zeturf Ltd" n'apparaît qu'au 16 juin 2005 ;

Qu'à la date du 28 juin 2005 - lendemain de la délivrance de l'assignation - le site n'était plus accessible par l'adresse "zeturf.fr", alors que suivant le constat dressé le 21 juin précédent le nom de domaine était toujours enregistré au nom de la société Zeturf.com à Paris, cette adresse redirigeant alors vers l'adresse "zeturf.com" ;

Attendu ceci exposé qu'il convient de rappeler que cette juridiction n'est pas liée par le type de mesures demandé ; que le caractère provisoire s'attachant à celles-ci commande de faire choix de celle qui se trouve à la fois nécessaire et suffisante ;

Qu'il apparaît avec une évidence suffisante à cette juridiction que les intérêts respectifs de la société Eturf et de la société Zeturf Ltd restent à tout le moins intimement liés, la première, en difficultés suivant ses écritures, tirant manifestement l'essentiel de ses ressources financières des redevances mensuelles versées par la seconde pour la fourniture du contenu nécessaire à la prise de paris en ligne ;

Que surtout, elle ne peut ignorer qu'elle fournit de manière générale et moyennant rémunération du contenu, et se trouve notamment amenée à procurer à la société Zeturf Ltd des renseignements sur les chances des chevaux de gagner les courses dans lesquelles ils sont engagés ; qu'il n'est pas sérieusement contestable qu'elle facilite ainsi de manière générale l'exploitation de la prise de paris ;

Qu'elle ne peut dès lors disconvenir que partie au moins de son activité continue de participer, alors que l'architecture du site et notamment sa charte graphique est restée identique, sauf modifications rendues nécessaires pour la création des rubriques permettant d'enregistrer les paris, du trouble à caractère manifestement illicite généré par cette activité de communication au public en ligne ;

Qu'elle ne peut donc être suivie en ses demandes tendant à débouter le PMU de

ses demandes en ce qu'elles sont dirigées à son encontre, dès lors que le site est dorénavant voué à la prise de paris ;

Que toutefois, l'accès au site par l'adresse "zeturf.fr" ayant cessé, il lui sera ordonné de mettre en œuvre tous les moyens à sa disposition pour mettre fin à toute contribution de sa part à l'exploitation illicite telle que définie plus haut, à moins que la société Zeturf Ltd n'y ait mis fin elle-même ;

Que cette juridiction assortira ces injonctions d'astreintes ainsi qu'elles seront précisées au dispositif, le demandeur étant débouté du surplus de ses demandes ;

Qu'il apparaîtrait inéquitable de laisser au PMU la charge des frais irrépétibles ;

Que les sociétés Eturf et Zeturf Ltd seront in solidum condamnées à lui payer la somme de 5000 € à ce titre ;

Statuant par mise à disposition au greffe, par ordonnance réputée contradictoire et en premier ressort,

Vu les dispositions de l'article 809 § 1 du ncpc,

. Constatons le trouble manifestement illicite résultant de l'activité de prise de paris organisée par le service de communication au public en ligne accessible à l'adresse "www.zeturf.com" ;

. Ordonnons à la société Zeturf Ltd de mettre fin à cette adresse à l'activité de prise de paris en ligne sur les courses hippiques organisées en France, et ce sous astreinte provisoire de 15 000 € par jour de retard à l'expiration du délai de 48 heures faisant suite à la signification de la présente décision ;

. Ordonnons à la société Eturf de mettre en œuvre tous moyens à sa disposition pour mettre fin à toute contribution à l'exploitation de la prise de paris en ligne sur le site en question, et ce sous astreinte provisoire de 8000 € par jour de retard faisant suite à l'expiration d'un délai de 48 heures suivant la signification de la présente décision ;

. Déboutons le PMU du surplus de ses demandes ;

. Condamnons les sociétés Eturf et Zeturf Ltd in solidum à payer au PMU la somme de 5000 € en application des dispositions de l'article 700 du ncpc ;

. Laissons les dépens in solidum à leur charge.

Que les dépens seront laissés in solidum à leur charge.

Référence : Tribunal de grande instance de Paris, ordonnance de référé du 08 juillet 2005, *PMU C/ ETURF*, *ZETURF*, DROIT-TIC
http://www.droit-tic.com/juris/aff.php?id_juris=33

C.N.I.L, délibération du 26 mai 2005, N° 2005-110, RELATIVE À UNE DEMANDE D'AUTORISATION DE MCDONALD'S FRANCE POUR LA MISE EN OEUVRE D'UN DISPOSITIF D'INTÉGRITÉ PROFESSIONNELLE

Thèmes
Informatique et libertés, droit social, droit du travail
Abstract
Informatique et Libertés, ligne éthique, surveillance du salarié, fichier d'alerte, autorisation (non)
Résumé
La société McDonald's France a saisi la CNIL afin de pouvoir mettre en oeuvre un dispositif "d'intégrité professionnelle"
Décision

La Commission nationale de l'informatique et des libertés,

Saisie le 7 janvier 2005 d'une déclaration portant sur la mise en oeuvre d'un dispositif d'intégrité professionnelle au sein du groupe McDonald's France,

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,

Après avoir entendu M. Hubert Bouchet, commissaire, en son rapport, et Mme Charlotte-Marie Pitrat, commissaire du Gouvernement, en ses observations,

Formule les observations suivantes ;

Sur le dispositif présenté

La société McDonald's France a saisi la CNIL afin de pouvoir mettre en oeuvre un dispositif "d'intégrité professionnelle".

Ce dispositif, qui s'inscrit dans le cadre du "code d'éthique" du groupe international McDonald's, permettrait aux collaborateurs des filiales françaises du groupe d'alerter, par courrier postal ou par télécopie, la société-mère américaine (McDonald's Corporation) sur les comportements de leurs collègues de travail "supposés contraires aux règles légales françaises ainsi qu'au code d'éthique".

Ce projet ne viserait que les agissements d'une partie des employés de McDonald's France, à savoir l'ensemble des collaborateurs du siège et les seuls cadres des cent soixante-quinze restaurants du groupe, soit environ mille personnes.

L'utilisation de ce dispositif, bien que prévue dans le code d'éthique du groupe, ne constituerait pas une obligation pesant sur les collaborateurs. Ces derniers en seraient clairement informés.

Le contenu des alertes transmises au service éthique de McDonald's Corporation aux Etats-Unis sous forme de courriers postaux ou de télécopies serait enregistré dans un fichier central placé sous la responsabilité du directeur éthique de cette

société. Chaque dossier enregistré dans ce fichier serait identifié par un numéro d'alerte pour assurer la confidentialité des informations.

Le directeur éthique de la maison-mère communiquerait au directeur juridique de McDonald's France, par courrier électronique protégé par un mot de passe, le contenu des courriers ou télécopies reçus. Ces données seraient ensuite orientées, en fonction de la nature de l'alerte, vers le responsable de service compétent selon le schéma suivant défini par McDonald's directeur des ressources humaines (pour les alertes relatives au droit social : présomption de harcèlement, de consommation d'alcool sur le lieu de travail, de discrimination, de décomptes d'horaires incohérents, autres sujets de préoccupation ayant trait à la conduite sur le lieu de travail), directeur de la sécurité (présomption d'un comportement susceptible d'être considéré comme un détournement de fonds, vol présumé de biens de la société, espionnage ou sabotage, corruption, diffusion ou divulgation d'informations confidentielles), directeur comptabilité et finances (audits de contrôle interne, irrégularités financières, pratiques contestables en matière comptable) ou autre destinataire (en fonction de la nature de la violation alléguée).

Le responsable de service déciderait d'ouvrir ou non une enquête et ne transmettrait la fiche d'alerte, le cas échéant, que vers les personnes qui devraient prendre part aux investigations. Il en informerait le directeur juridique de McDonald's France et le consulterait pour diligenter l'enquête.

En cas de mise en cause d'un membre de la direction générale de McDonald's France, l'enquête serait conduite directement par la maison-mère américaine.

Le fichier d'alerte utilisé pour l'enquête comporterait les données suivantes : nom, prénom et ville de résidence de l'expéditeur du courrier (si la personne décline son identité), nom du restaurant ou des bureaux, fonctions exercées par l'expéditeur du courrier, nom et prénom de la personne visée par l'allégation de non-respect du code d'éthique, ou nom et prénom d'un autre collaborateur qui pourrait avoir connaissance des faits le cas échéant, nature des allégations, conclusions de l'enquête (classement du dossier sans suite, type de sanctions prises, autres actions correctives).

Les collaborateurs présumés fautifs seraient informés de leurs droits d'accès, de rectification et d'opposition dans un délai de deux jours ouvrables par le directeur des ressources humaines, même s'il n'était procédé à aucune enquête.

Le résultat de l'enquête et les "mesures correctives" prises (modification des contrôles internes ou d'autres règles en vigueur au sein du groupe français, sanctions disciplinaires, actions en justice) seraient transmis, sans l'identité de l'employé concerné, par le directeur juridique de McDonald's France au directeur éthique de McDonald's Corporation.

Les données des fiches d'alerte informatisées seraient conservées par McDonald's France, en cas de comportement fautif retenu par l'enquête, entre une et cinq années en fonction de la nature de la faute commise. Le directeur juridique, le directeur des ressources humaines, le responsable hiérarchique du collaborateur concerné et un membre de la direction générale auraient la possibilité d'y accéder.

Les fiches d'alerte ne donnant pas lieu à enquête ou pour lesquelles l'enquête

s'avèrerait négative seraient détruites dans les deux jours ouvrables après la décision de clôture.

Enfin, les fiches d'alerte détenues par le service éthique de McDonald's Corporation ne seraient pas conservées au-delà de trois mois à l'issue de la conclusion de l'enquête et de cinq années pour celles concernant les membres de la direction générale de McDonald's France.

Un contrat de flux transfrontières concernant les échanges de données personnelles entre la France et les Etats-Unis a été signé entre la société-mère et sa filiale française.

Sur la détermination du responsable de traitement et l'application de la loi du 6 janvier 1978

L'article 3 de la loi du 6 janvier 1978 modifiée dispose que le responsable d'un traitement de données à caractère personnel est, sauf désignation expresse par les dispositions législatives ou réglementaires relatives à ce traitement, la personne, l'autorité publique, le service ou l'organisme qui détermine ses finalités et ses moyens.

Il ressort du dossier de formalités préalables présenté par la société McDonald's France que cette dernière agit auprès de la CNIL en qualité de responsable du dispositif d'intégrité professionnelle qu'elle envisage de mettre en oeuvre, et en particulier des traitements de données opérés lors des enquêtes diligentées sur des employés déterminés à la suite d'un signalement opéré dans le cadre du dispositif.

Au-delà, l'incitation à utiliser ce dispositif, présente dans le "code d'éthique" établi par la société McDonald's France et les adaptations substantielles apportées par cette société, durant l'instruction du dossier, au dispositif initialement envisagé (suppression des projets de ligne téléphonique et d'adresse électronique dédiées au dispositif d'intégrité professionnelle) caractérisent la responsabilité de cette société sur le traitement de données personnelles envisagé au regard de l'article 3 de la loi précitée.

L'existence d'un contrat de flux transfrontières de données personnelles (de responsable de traitement à responsable de traitement) avec la société McDonald's Corporation constitue un élément supplémentaire en ce sens.

La Commission constate en conséquence que la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés est applicable au dispositif d'intégrité professionnelle présenté et qu'elle est donc compétente pour se prononcer sur la conformité du projet à cette loi.

Sur la procédure déclarative applicable

La Commission relève que le dispositif envisagé peut dans certains cas conduire le groupe McDonald's France à décider, au titre des "mesures correctives" qu'il doit prendre à la suite d'une alerte, à exclure des employés considérés fautifs du bénéfice de leur contrat de travail en l'absence de toute disposition législative ou réglementaire encadrant ce type de traitement.

Dès lors, la procédure d'autorisation prévue à l'article 25-I, 4° de la loi du 6 janvier 1978 modifiée doit être appliquée au traitement de données personnelles présenté.

Sur la conformité du dispositif présenté à la loi du 6 janvier 1978

La Commission considère que la mise en oeuvre par un employeur d'un dispositif destiné à organiser auprès de ses employés le recueil, quelle qu'en soit la forme, de données personnelles concernant des faits contraires aux règles de l'entreprise ou à la loi imputables à leurs collègues de travail, en ce qu'il pourrait conduire à un système organisé de délation professionnelle, ne peut qu'appeler de sa part une réserve de principe au regard de la loi du 6 janvier 1978 modifiée, et en particulier de son article 1er.

En ce sens, la Commission observe que la possibilité de réaliser une "alerte éthique" de façon anonyme ne pourrait que renforcer le risque de dénonciation calomnieuse.

Au surplus, la Commission estime que le dispositif présenté est disproportionné au regard des objectifs poursuivis et des risques de dénonciations calomnieuses et de stigmatisation des employés objets d'une "alerte éthique". Elle relève à cet égard que d'autres moyens prévus par la loi existent d'ores et déjà afin de garantir le respect des dispositions légales et des règles fixées par l'entreprise (actions de sensibilisation par l'information et la formation des personnels, rôle d'audit et d'alerte des commissaires aux comptes en matière financière et comptable, saisine de l'inspection du travail ou des juridictions compétentes).

La Commission relève enfin que les employés objets d'un signalement ne seraient, par définition, pas informés dès l'enregistrement de données mettant en cause leur intégrité professionnelle ou de citoyen, et n'auraient donc pas les moyens de s'opposer à ce traitement de données les concernant. Les modalités de collecte et de traitement de ces données, dont certaines pourraient concerner des faits susceptibles d'être constitutifs d'infractions pénales, ne peuvent dès lors être considérées comme loyales au sens de l'article 6 de la loi du 6 janvier 1978 modifiée.

Compte tenu de ces observations, la Commission n'autorise pas la mise en oeuvre du dispositif d'intégrité professionnelle présenté par la société McDonald's France.

Le président, Alex TURK.

Caractère de la délibération : Refus d'autorisation
Traités cités : Convention 1981-01-28 pour la protection des personnes à l'égard du traitement automatisé des données à caractère, convention du Conseil de l'Europe. Directive 95-46 1995-10-24
Lois citées : Loi 78-17 1978-01-06 art. 25, art. 3, art. 1er, art. 6. Loi 2004-801 2004-08-06.

Référence : C.N.I.L, délibération du 26 mai 2005, *N° 2005-110, RELATIVE À UNE DEMANDE D'AUTORISATION DE MCDONALD'S FRANCE POUR LA MISE EN OEUVRE D'UN DISPOSITIF D'INTÉGRITÉ PROFESSIONNELLE*, DROIT-TIC
http://www.droit-tic.com/juris/aff.php?id_juris=32

C.N.I.L, délibération du 26 mai 2005, N° 2005-111 RELATIVE À UNE DEMANDE D'AUTORISATION DE LA COMPAGNIE EUROPÉENNE D'ACCUMULATEURS POUR LA MISE EN OEUVRE D'UN DISPOSITIF DE "LIGNE ETHIQUE"

Thèmes
Informatique et libertés, droit social, droit du travail
Abstract
Informatique et Libertés, violations des principes en vigueur dans l'entreprise, comité de surveillance comptable du conseil d'administration, autorisation (non)
Résumé
La "hotline" devrait également permettre aux salariés d'alerter les dirigeants du groupe sur les éventuelles violations des principes en vigueur dans l'entreprise
Décision

La Commission nationale de l'informatique et des libertés,

Saisie le 29 juillet 2004 d'une déclaration portant sur la mise en oeuvre d'un dispositif de "ligne éthique" au sein de la Compagnie européenne d'accumulateurs,

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,

Après avoir entendu M. Hubert Bouchet, commissaire, en son rapport, et Mme Charlotte-Marie Pitrat, commissaire du Gouvernement, en ses observations,

Formule les observations suivantes :

Sur le dispositif présenté

La Compagnie européenne d'accumulateurs (CEAC) a saisi la CNIL d'une déclaration concernant la mise en oeuvre d'une "hotline" (ligne téléphonique dédiée) à destination de ses 1500 employés.

Ce dispositif de "ligne éthique", conçu par sa société mère Exide Technologies afin de se conformer aux dispositions de la loi américaine dite "Sarbanes-Oxley", devrait permettre à l'ensemble des salariés du groupe "de communiquer avec le comité de surveillance comptable du conseil d'administration d'Exide sur des sujets tels que les inexactitudes ou les irrégularités comptables qui pourraient être commises".

La "hotline" devrait également permettre aux salariés d'alerter les dirigeants du groupe sur les éventuelles violations des principes en vigueur dans l'entreprise (règles de conduite éthique ou commerciale) ou des lois en vigueur.

Le dispositif s'appuierait à la fois sur un numéro vert et sur une adresse électronique.

Dans les deux cas, les alertes et les demandes d'information seraient en fait

adressées à un sous-traitant américain pour le compte de Exide Technologies. S'agissant des appels passés en langue française, un second prestataire de service américain interviendrait.

S'il le souhaitait, l'anonymat de l'appelant serait garanti.

Les sous-traitants seraient chargés d'enregistrer sur support informatique le contenu des demandes et des alertes selon la classification suivante : "(1) ressources humaines ou problèmes de travail, (2) fraude ou vol, (3) erreur comptable, (4) problèmes liés aux principes de conduite et d'éthique".

En fonction de cette classification, un résumé écrit des appels et des messages électroniques reçus devrait ensuite être transmis, par e-mail crypté, aux personnes nommément désignées à cet effet par la société-mère (département juridique, département comptabilité, comité international, comité de vérification des comptes du conseil d'administration).

Le destinataire de l'information au sein d'Exide Technologies réaliserait ensuite, le cas échéant, une enquête interne. Celle-ci s'effectuerait en liaison avec le responsable juridique France (CEAC) qui recevrait les données nécessaires par courrier électronique.

Un "suivi de dossier" serait également adressé, par voie électronique, par la société-mère au responsable juridique France, qui le transmettrait au responsable des ressources humaines France.

Tout salarié concerné par un appel serait informé "le plus tôt possible des allégations prononcées à son encontre de telle sorte qu'il puisse s'expliquer".

Enfin, la durée de conservation des données serait limitée à une année.

Sur la détermination du responsable de traitement et l'application de la loi du 6 janvier 1978

L'article 3 de la loi du 6 janvier 1978 modifiée dispose que le responsable d'un traitement de données à caractère personnel est, sauf désignation expresse par les dispositions législatives ou réglementaires relatives à ce traitement, la personne, l'autorité publique, le service ou l'organisme qui détermine ses finalités et ses moyens.

Il ressort du dossier de formalités préalables présenté par la société CEAC que cette dernière agit auprès de la CNIL en qualité de responsable du dispositif de "ligne éthique" qu'elle envisage de mettre en oeuvre, et en particulier des traitements de données opérés lors des enquêtes diligentées sur des employés déterminés à la suite d'un signalement opéré dans le cadre du dispositif.

Dès lors, la Commission constate que la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés est applicable au dispositif de "ligne éthique" présenté et qu'elle est donc compétente pour se prononcer sur la conformité du projet à cette loi.

Sur la procédure déclarative applicable

La Commission relève que le dispositif envisagé est susceptible de conduire la société CEAC à décider, au titre des mesures correctives qu'elle doit prendre à la suite d'un signalement, à exclure des employés considérés fautifs du bénéfice de leur contrat de travail en l'absence de toute disposition législative ou réglementaire encadrant ce type de traitement.

Dès lors, la procédure d'autorisation prévue à l'article 25-1, 4° de la loi du 6 janvier

1978 modifiée doit être appliquée au traitement de données personnelles présenté.

Sur la conformité du dispositif présenté à la loi du 6 janvier 1978

La Commission considère que la mise en oeuvre par un employeur d'un dispositif destiné à organiser auprès de ses employés le recueil, quelle qu'en soit la forme, de données personnelles concernant des faits contraires aux règles de l'entreprise ou à la loi imputables à leurs collègues de travail, en ce qu'il pourrait conduire à un système organisé de délation professionnelle, ne peut qu'appeler de sa part une réserve de principe au regard de la loi du 6 janvier 1978 modifiée, et en particulier de son article 1er.

En ce sens, la Commission observe que la possibilité de réaliser une "alerte éthique" de façon anonyme ne pourrait que renforcer le risque de dénonciation calomnieuse.

Au surplus, la Commission estime que le dispositif présenté est disproportionné au regard des objectifs poursuivis et des risques de dénonciations calomnieuses et de stigmatisation des employés objets d'une "alerte éthique". Elle relève à cet égard que d'autres moyens prévus par la loi existent d'ores et déjà afin de garantir le respect des dispositions légales et des règles fixées par l'entreprise (actions de sensibilisation par l'information et la formation des personnels, rôle d'audit et d'alerte des commissaires aux comptes en matière financière et comptable, saisine de l'inspection du travail ou des juridictions compétentes).

La Commission relève enfin que les employés objets d'un signalement ne seraient, par définition, pas informés dès l'enregistrement de données mettant en cause leur intégrité professionnelle ou de citoyen, et n'auraient donc pas les moyens de s'opposer à ce traitement de données les concernant. Les modalités de collecte et de traitement de ces données, dont certaines pourraient concerner des faits susceptibles d'être constitutifs d'infractions pénales, ne peuvent dès lors être considérées comme loyales au sens de l'article 6 de la loi du 6 janvier 1978 modifiée.

Compte tenu de ces observations, la Commission n'autorise pas la mise en oeuvre du dispositif de "ligne éthique" présenté par la Compagnie européenne d'accumulateurs.

Le président, Alex TURK.

Caractère de la délibération : Refus d'autorisation
Traités cités : Convention 1981-01-28 pour la protection des personnes à l'égard du traitement automatisé des données à caractère, convention du Conseil de l'Europe. Directive 95-46 1995-10-24
Lois citées : Loi 78-17 1978-01-06 art. 25, art. 3, art. 1er, art. 6. Loi 2004-801 2004-08-06.

Référence : C.N.I.L, délibération du 26 mai 2005, *N° 2005-111 RELATIVE À UNE DEMANDE D'AUTORISATION DE LA COMPAGNIE EUROPÉENNE D'ACCUMULATEURS POUR LA MISE EN OEUVRE D'UN DISPOSITIF DE "LIGNE ETHIQUE"*, DROIT-TIC http://www.droit-tic.com/juris/aff.php?id_juris=31

C.N.I.L, délibération du 26 mai 2005, N° 2005-111 RELATIVE À UNE DEMANDE D'AUTORISATION DE LA COMPAGNIE EUROPÉENNE D'ACCUMULATEURS POUR LA MISE EN OEUVRE D'UN DISPOSITIF DE "LIGNE ETHIQUE"

Thèmes
Informatique et libertés, droit social, droit du travail
Abstract
Informatique et Libertés, violations des principes en vigueur dans l'entreprise, comité de surveillance comptable du conseil d'administration, autorisation (non)
Résumé
La "hotline" devrait également permettre aux salariés d'alerter les dirigeants du groupe sur les éventuelles violations des principes en vigueur dans l'entreprise
Décision

La Commission nationale de l'informatique et des libertés,

Saisie le 29 juillet 2004 d'une déclaration portant sur la mise en oeuvre d'un dispositif de "ligne éthique" au sein de la Compagnie européenne d'accumulateurs,

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,

Après avoir entendu M. Hubert Bouchet, commissaire, en son rapport, et Mme Charlotte-Marie Pitrat, commissaire du Gouvernement, en ses observations,

Formule les observations suivantes :

Sur le dispositif présenté

La Compagnie européenne d'accumulateurs (CEAC) a saisi la CNIL d'une déclaration concernant la mise en oeuvre d'une "hotline" (ligne téléphonique dédiée) à destination de ses 1500 employés.

Ce dispositif de "ligne éthique", conçu par sa société mère Exide Technologies afin de se conformer aux dispositions de la loi américaine dite "Sarbanes-Oxley", devrait permettre à l'ensemble des salariés du groupe "de communiquer avec le comité de surveillance comptable du conseil d'administration d'Exide sur des sujets tels que les inexactitudes ou les irrégularités comptables qui pourraient être commises".

La "hotline" devrait également permettre aux salariés d'alerter les dirigeants du groupe sur les éventuelles violations des principes en vigueur dans l'entreprise (règles de conduite éthique ou commerciale) ou des lois en vigueur.

Le dispositif s'appuierait à la fois sur un numéro vert et sur une adresse électronique.

Dans les deux cas, les alertes et les demandes d'information seraient en fait

adressées à un sous-traitant américain pour le compte de Exide Technologies. S'agissant des appels passés en langue française, un second prestataire de service américain interviendrait.

S'il le souhaitait, l'anonymat de l'appelant serait garanti.

Les sous-traitants seraient chargés d'enregistrer sur support informatique le contenu des demandes et des alertes selon la classification suivante : "(1) ressources humaines ou problèmes de travail, (2) fraude ou vol, (3) erreur comptable, (4) problèmes liés aux principes de conduite et d'éthique".

En fonction de cette classification, un résumé écrit des appels et des messages électroniques reçus devrait ensuite être transmis, par e-mail crypté, aux personnes nommément désignées à cet effet par la société-mère (département juridique, département comptabilité, comité international, comité de vérification des comptes du conseil d'administration).

Le destinataire de l'information au sein d'Exide Technologies réaliserait ensuite, le cas échéant, une enquête interne. Celle-ci s'effectuerait en liaison avec le responsable juridique France (CEAC) qui recevrait les données nécessaires par courrier électronique.

Un "suivi de dossier" serait également adressé, par voie électronique, par la société-mère au responsable juridique France, qui le transmettrait au responsable des ressources humaines France.

Tout salarié concerné par un appel serait informé "le plus tôt possible des allégations prononcées à son encontre de telle sorte qu'il puisse s'expliquer".

Enfin, la durée de conservation des données serait limitée à une année.

Sur la détermination du responsable de traitement et l'application de la loi du 6 janvier 1978

L'article 3 de la loi du 6 janvier 1978 modifiée dispose que le responsable d'un traitement de données à caractère personnel est, sauf désignation expresse par les dispositions législatives ou réglementaires relatives à ce traitement, la personne, l'autorité publique, le service ou l'organisme qui détermine ses finalités et ses moyens.

Il ressort du dossier de formalités préalables présenté par la société CEAC que cette dernière agit auprès de la CNIL en qualité de responsable du dispositif de "ligne éthique" qu'elle envisage de mettre en oeuvre, et en particulier des traitements de données opérés lors des enquêtes diligentées sur des employés déterminés à la suite d'un signalement opéré dans le cadre du dispositif.

Dès lors, la Commission constate que la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés est applicable au dispositif de "ligne éthique" présenté et qu'elle est donc compétente pour se prononcer sur la conformité du projet à cette loi.

Sur la procédure déclarative applicable

La Commission relève que le dispositif envisagé est susceptible de conduire la société CEAC à décider, au titre des mesures correctives qu'elle doit prendre à la suite d'un signalement, à exclure des employés considérés fautifs du bénéfice de leur contrat de travail en l'absence de toute disposition législative ou réglementaire encadrant ce type de traitement.

Dès lors, la procédure d'autorisation prévue à l'article 25-1, 4° de la loi du 6 janvier

1978 modifiée doit être appliquée au traitement de données personnelles présenté.

Sur la conformité du dispositif présenté à la loi du 6 janvier 1978

La Commission considère que la mise en oeuvre par un employeur d'un dispositif destiné à organiser auprès de ses employés le recueil, quelle qu'en soit la forme, de données personnelles concernant des faits contraires aux règles de l'entreprise ou à la loi imputables à leurs collègues de travail, en ce qu'il pourrait conduire à un système organisé de délation professionnelle, ne peut qu'appeler de sa part une réserve de principe au regard de la loi du 6 janvier 1978 modifiée, et en particulier de son article 1er.

En ce sens, la Commission observe que la possibilité de réaliser une "alerte éthique" de façon anonyme ne pourrait que renforcer le risque de dénonciation calomnieuse.

Au surplus, la Commission estime que le dispositif présenté est disproportionné au regard des objectifs poursuivis et des risques de dénonciations calomnieuses et de stigmatisation des employés objets d'une "alerte éthique". Elle relève à cet égard que d'autres moyens prévus par la loi existent d'ores et déjà afin de garantir le respect des dispositions légales et des règles fixées par l'entreprise (actions de sensibilisation par l'information et la formation des personnels, rôle d'audit et d'alerte des commissaires aux comptes en matière financière et comptable, saisine de l'inspection du travail ou des juridictions compétentes).

La Commission relève enfin que les employés objets d'un signalement ne seraient, par définition, pas informés dès l'enregistrement de données mettant en cause leur intégrité professionnelle ou de citoyen, et n'auraient donc pas les moyens de s'opposer à ce traitement de données les concernant. Les modalités de collecte et de traitement de ces données, dont certaines pourraient concerner des faits susceptibles d'être constitutifs d'infractions pénales, ne peuvent dès lors être considérées comme loyales au sens de l'article 6 de la loi du 6 janvier 1978 modifiée.

Compte tenu de ces observations, la Commission n'autorise pas la mise en oeuvre du dispositif de "ligne éthique" présenté par la Compagnie européenne d'accumulateurs.

Le président, Alex TURK.

Caractère de la délibération : Refus d'autorisation
Traités cités : Convention 1981-01-28 pour la protection des personnes à l'égard du traitement automatisé des données à caractère, convention du Conseil de l'Europe. Directive 95-46 1995-10-24
Lois citées : Loi 78-17 1978-01-06 art. 25, art. 3, art. 1er, art. 6. Loi 2004-801 2004-08-06.

Référence : C.N.I.L, délibération du 26 mai 2005, *N° 2005-111 RELATIVE À UNE DEMANDE D'AUTORISATION DE LA COMPAGNIE EUROPÉENNE D'ACCUMULATEURS POUR LA MISE EN OEUVRE D'UN DISPOSITIF DE "LIGNE ETHIQUE"*, DROIT-TIC http://www.droit-tic.com/juris/aff.php?id_juris=31