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

ANALYSES

DECRETS

DECISIONS ARCEP

DROIT-TIC.COM

© Julien Le Clainche

RDTIC

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

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

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

Conseil scientifique

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

Informations légales

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

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

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

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

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

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

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

© Julien Le Clainche

DROIT-TIC .com

R.D.T.I.C

LA REVUE DU DROIT DES TECHNIQUES DE L'INFORMATION ET DE LA COMMUNICATION-
N°60 – JANVIER 2007

ANALYSES

DÉCRET

DÉCISION ARCEP

DROIT-TIC .com

R.D.T.I.C

LA REVUE DU DROIT DES TECHNIQUES DE L'INFORMATION ET DE LA COMMUNICATION-
N°60 – JANVIER 2007

ÉCONOMIE NUMÉRIQUE, RESPONSABILITÉ

DE LA PRESCRIPTION À TRÈS HAUT DÉBIT OU DE L'URGENCE D'AGIR ?

Par Me. Xavier Hofman, Avocat

Disposition peu ou mal connue du Code des Postes et Communications Électroniques, l'article L.34-2 édicte un (très) court délai de prescription des sommes dues aux FAI et aux opérateurs télécom.

Disposition peu ou mal connue du Code des Postes et Communications Électroniques, l'article L.34-2 édicte un (très) court délai de prescription des sommes dues aux FAI et aux opérateurs télécom.

Par ailleurs, les modalités de suspension de ce délai sont peu nombreuses et les conditions générales des prestataires ont tendance à étendre ce délai à toute forme d'actions en responsabilité (ex. : en cas de défaut de qualité de service).

Les clients-entreprises doivent s'assurer, lors de la négocation de leurs accords, d'un équilibre des relations à l'égard de la prescription.

De la prescription à « très haut débit » ou de l'urgence d'agir ?

Parmi les dispositions légales peut-être méconnues des relations entre opérateurs télécom, FAI et utilisateurs figure celle relative à la prescription en matière de prestation de communications électroniques.

L'ancien article L.126 du Code des Postes et Télécommunications, devenu l'article L.34-2 du Code des Postes et Communications Électroniques (CPCE), édicte un bref délai d'un an pour discuter du prix facturé par les prestataires.

En d'autres termes, les clients disposent d'un délai d'un an pour réclamer le remboursement des sommes qu'ils estiment indûment versées et les opérateurs « L.33-1 » du même délai pour réclamer le paiement des sommes dues.

L'article L.34-2, de rédaction ancienne, voire ambiguë sous certains aspects (cf. notamment la notion *« d'usager »* du 2ième alinéa), a pourtant subi un « léger » toilettage en 2004 quant à son champ d'application. Longtemps cantonné aux relations entre les opérateurs télécom et leurs abonnés, cet article est désormais également applicable aux relations entre les fournisseurs d'accès internet (FAI) et leurs clients.

Quant aux services concernés, l'article L.34-2 est applicable aux seules prestations de communications électroniques, c'est-à-dire, selon le 1° de l'article L.32 CPCE, aux *« émissions, transmissions ou réceptions de signes, de signaux, d'écrits, d'images ou de sons, par voie électromagnétique »*. Toutefois, sont exclues les prestations *« consistant à éditer ou à distribuer des services de communication au public par voie électronique »* (prestations de contenu).

Au-delà d'un an, il n'est donc plus possible de contester efficacement les sommes facturées et les versements effectués. Pour les clients, le délai commence à courir à compter de la date d'exigibilité des montants dus. Pour les opérateurs et les FAI, il démarre à compter du jour du paiement du prix de leurs prestations.

En comparaison avec les autres délais de prescription du domaine commercial, ce délai est très court.

Du point de vue des clients-particuliers, ce trop bref délai, souvent passé inaperçu, risque de les empêcher de faire utilement valoir leurs droits et jouera, par conséquent, contre leurs intérêts ce qui n'a jamais été l'objectif du législateur.

Du point de vue des clients-entreprises, ce trop bref délai porte en germe le risque d'une crispation rapide des tentatives de règlement amiable des litiges. En d'autres termes, clients et prestataires risquent d'être rapidement tentés par l'aventure contentieuse afin de préserver leurs droits, au détriment – nécessairement – de l'avenir de leur relation commerciale.

Et ce, d'autant plus que les textes se montrent très stricts à l'égard des possibilités d'interruption de ce délai. En substance et parmi les causes d'interruption, figurent essentiellement la reconnaissance par le débiteur de sa dette, la signification de l'ordonnance d'injonction de payer et l'assignation au fond. Si les deux premières causes semblent exploitables par les prestataires, seule l'assignation au fond dans le délai d'un an paraît pertinente pour les clients.

On pourra objecter cependant que ce bref délai se révèle favorable aux clients et à leurs prestataires en ce sens

qu'il coïncide opportunément avec le délai de l'article L.34-1 CPCE au terme duquel les opérateurs et les FAI doivent effacer ou rendre anonymes les données de trafic concernant leurs clients.

Toutefois, outre que cela n'enlève rien à la brièveté du délai, la rédaction de l'article L.34-2 révèle que la prescription qu'il édicte ne s'applique qu'aux litiges relatifs au prix des prestations : tout autre manquement relevant de la responsabilité demeure, par conséquent, hors du champ de cette prescription spéciale. Il en sera ainsi des revendications fondées, par exemple, sur un défaut de qualité de service. Les actions qui en découlent devraient normalement relever de la prescription de droit commun, soit dix ans en matière commerciale et trente ans en matière civile. À cet égard, on peut s'interroger néanmoins sur les modalités d'administration de la preuve en cas de litige né au-delà de l'expiration du délai d'un an confrontée à l'obligation faite aux prestataires, et rappelée ci-dessus, d'effacer ou de rendre anonymes les données de communication. Dans ce cas, la coïncidence des délais d'un an des articles L.34-1 et L.34-2 risquent de jouer au détriment de l'ensemble des parties.

En pratique, les prescriptions n'étant pas d'ordre public, les conditions générales et contrats proposés par les opérateurs télécom et les FAI tendent à assimiler tous types d'actions à la prescription d'un an de l'article L.34-2. En outre et pour le même motif, les dérogations négociées dans le cadre des accords avec les clients sont possibles. La durée du délai peut être allongée ou il peut être valablement stipulé qu'une mise en demeure, par voie recommandée avec demande d'avis de réception postale, par exemple, suffit à interrompre le délai de prescription.

Dans ces conditions, on ne saurait que trop conseiller aux clients-entreprises de négocier *a minima* la réciprocité des clauses relatives à la prescription qui émaillent, le plus souvent à sens unique, les contrats et conditions générales de leurs prestataires. Une telle discussion sera opportunément lancée à l'occasion de la négociation de la clause de responsabilité dont le délai de prescription constitue finalement l'un des aspects structurants : que vaudrait, en effet, une excellente clause de responsabilité enserrée dans un trop bref délai de mise en œuvre ?

Quant aux clients-particuliers, en l'absence d'un geste commercial volontaire ou favorisé, dans certains cas, par le recours à la médiation, il ne leur reste le plus souvent que la voie de l'assignation au fond, c'est-à-dire celle du procès. Gageons qu'ils risquent d'être faiblement tentés par ce mode de règlement de leurs différends, peu en phase avec leurs enjeux. Mis en regard des difficultés que semblent rencontrer les particuliers avec leurs opérateurs et FAI, le peu de contentieux généré, vaguement camouflé par quelques retentissantes affaires, ne serait alors que le révélateur d'une frustration, propice à l'intervention législative ou réglementaire souvent peu empreinte de souplesse.

En conclusion, peut-être serait-il temps de s'interroger sur la permanence du bref délai de l'article L.34-2 : une telle dérogation aux règles habituelles du commerce demeure-t-elle justifiée ?

On se souviendra qu'elle avait été voulue, initialement, pour éviter le stockage trop lourd des données de télécommunications, qu'elle interagit toujours avec les délais de conservation des données de trafic, mais dans un objectif de protection du client cette fois. On l'a vu, il n'est pas certain que le dispositif satisfasse véritablement à cet objectif pourtant essentiel.

On militera pour le moins en faveur d'une révision textuelle achevant de lever toute ambiguïté, notamment au travers d'une rédaction symétrique avec les dispositions applicables au secteur postal (cf. article 11 CPCE).

À une époque où le droit des communications électroniques tend à s'incorporer au droit commercial, peut-être serait-il temps d'en tirer également les conséquences au regard de la prescription.

Xavier HOFMAN (www.cosich-avocats.com)

R.D.T.I.C
LA REVUE DU DROIT DES TECHNIQUES DE L'INFORMATION ET DE LA COMMUNICATION-
N°60 – JANVIER 2007

NOMS DE DOMAINE, PROPRIÉTÉ INDUSTRIELLE

INTERVIEW EXCLUSIVE DU REGISTRE DOTASIA

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

Leona Chen, membre du DotAsia, en charge des relations avec les « registrars », a accordé à MailClub.info, une interview exclusive.

2007 sera l'année du .asia. Afin de tout comprendre sur cette nouvelle extension, MailClub.info publie un dossier d'actualité à ce sujet (pour l'obtenir, cliquez ici). Leona Chen, membre du DotAsia, en charge des relations avec les « registrars », a également accordé à MailClub.info, une interview exclusive. Dans un long entretien, elle nous raconte comment est né ce projet. Elle nous dévoile également les conditions d'enregistrements de cette extension, comment les « sunrise period » vont se dérouler, le fonctionnement des enchères pour certains noms de domaine, le calendrier de lancement de l'extension...

- MailClub.info : Racontez nous comment est né le projet du .asia ?

Leona Chen : *L'origine du projet remonte à l'année 2000 où ont commencées les discussions autour de l'intérêt de fonder un TLD régional. A la différence du .eu, il n'existe pas de d'organisation pan asiatique mais une myriade d'organisations régionales. Les discussions autour de l'intérêt de fonder un TLD pour l'Asie se sont poursuivies de manière informelle. Différentes organisations ont lancé des propositions, notamment la Kore qui proposait la création d'un .AS en tant que TLD.*

Fin 2002, durant la conférence ITU de HongKong, les discussions se sont intensifiées et se sont mêlées aux discussions menées par l'Icann au même moment autour de la création de nouveaux sTLD sponsorisés.

Tout au long de l'année 2003 les discussions se sont poursuivies. Parmi les participants actifs au projet, on compte Mr Chee-Hoo Cheng, qui participe depuis longtemps à la communauté internet en Asie et Edmon Chung, qui fait figure de pionnier en terme de promotion des IDN.

Le 15 décembre 2003, l'Icann a lancé un appel a proposition pour des TLD sponsorisés L'initiative s'est alors accélérée et a commencé a prendre forme. Par la suite, une structure pour une nouvelle organisation sponsorisée a vu le jour, celle ci étant ouverte à toute organisation de la région souhaitant y participer.

Cela a permis de réunir un large éventail de participants et de bénéficier d'une base solide de savoirs et de connaissances nécessaire a la gestion d'un registre de TLD. Quand la proposition a été remise a l'Icann le 16 mars 2004, on comptait parmi les membres participants, 7 cctlds (.cn, .id, .jp, .mo, .nu, .tw, and .vn) ainsi que l' Asia Pacific Network Information Centre (APNIC) et l' Asia Pacific Network Group (APNG). Depuis, de nouveaux membres se sont greffés. Il y a déjà 20 cctld qui participent (incluant notamment le .kz, .tj et .uz, .af, .bt, .in, .ir, . kh, .ph, .sg, .kr, .mn et .nz).

- Le .asia est il selon vous l'équivalent du .eu pour l'Union Européenne ?

A la différence du .eu, la création du .asia est partie d'une initiative commune qui n'était ni créée ni mandatée par aucun gouvernement ni aucune organisation existante. C'est le résultat d'une simple initiative qui s'est vue soutenue au fur et a mesure par un ensemble assez varié d'organisations bien implantées dans la région.

Une idendité régionale

- Quel est l'intérêt d'enregistrer un .asia pour une société qui aurait déjà plusieurs cctld asiatiques ?

Nous pensons que le .asia répond à deux besoins :
- *ceux du marché dans le cadre d'une communauté à forte croissance économique*
- *disposer d'un front commun capable d'améliorer notre reconnaissance internationale mais aussi d'acquérir une compétitivité régionale capable de peser sur l'échiquier mondial.*

Internet joue un rôle de plus en plus important dans le nouvel essor des économies pan asiatiques et d'asie-pacifique. Etant donné que les sociétés visent au delà de leurs économies locales, une identité régionale en ligne est fondamentale.

Quand des multinationales s'installent dans la région, elles ont besoin d'une identification régionale. Une simple identification locale ne suffit pas. Par exemple,

si une société installe son siège social à Shanghai, une adresse en .cn convient pour communiquer avec ses clients potentiels en Chine. Toutefois, quand cette même société se rend au Japon, une adresse en .asia permet de renforcer son champ de prospection.

Une adresse régionale permet aussi aux entreprises locales de se défaire de certains préjugés liés à leurs régions d'origine lorsqu'elles souhaitent s'attaquer à d'autres marchés. Le .asia répondra à la demande d'un "marché virtuel central" gommant les identités régionales, assurant ainsi la neutralité.

Comme dans la plupart des régions, le marché est constitué principalement par les PME. Nous pensons fermement que le segment des PME tirera le plus les bénéfices de la création du .asia.

- Quelles sont les conditions pour enregistrer un .asia ?

Pour enregistrer un .asia, le demandeur doit être une entité légale présente dans la région Asie / Australie / Pacifique telles que définies par l'Icann.

Sont autorisées à enregistrer un .asia :

- *toute organisation (société, association, groupes sociaux, etc) établie dans la communauté*
- *tout citoyen résident dans la communauté*
- *tout gouvernement / personne publique établie dans la communauté.*

- A qui sont dédiées les sunrise period ?

La première sunrise concernera les gouvernements et leurs entités associées. La seconde sera pour les titulaires de marques. Ensuite, l'ouverture sera totale du moment que le titulaire soit établi dans la région.

Des enchères pour les demandes multiples

- Comment vont fonctionner les enchères entre la sunrise 2 et le landrush ?

Les enchères auront lieu uniquement et seulement pour le cas de demandes multiples pour un même domaine. Les noms de domaine pour lesquels une seule demande valide a été déposée seront enregistrés. Les enchères ont lieu pour les domaines pour lesquels plusieurs demandes valides ont été déposées.

- Ne craignez-vous pas ainsi d'encourager le cybersquatting ?

C'est avec l'idée de décourager le cybersquatting que nous sommes parti sur l'idée des enchères. Comme nous l'avons expliqué, les enchères n'auront lieu qu'entre les demandeurs ayants déposé leur demande pendant la « sunrise » et le « landrush » et pour des domaines sur lesquels il a été préalablement vérifié qu'ils détenaient des droits antérieurs.

Ce système d'enchères permet de résoudre les problèmes techniques et la haute tension qu'engendre la règle habituelle du « premier arrivé, premier servi ». Nous sortons de la loterie.

Nous estimons que grâce au système des enchères le nom de domaine sera attribué à l'entité la plus a même d'utiliser et de développer une adresse en .asia.

- Pouvez-vous nous communiquer les dates de lancement du .asia ?

Voici notre calendrier :

- *Avril 2007 - Début de la sunrise 1*
- *Juin 2007 - Début de la sunrise 2 pour les titulaires de marques*
- *Septembre / Octobre 2007 - « Landrush »*
- *Octobre / Novembre 2007 - Enchères entre les demandes issues des sunrise 2 et des landrush*
- *Hiver 2007 - Ouverture à tous.*

- Attendez-vous beaucoup d'enregistrement de la part de sociétés américaines ou européennes ?

Il est difficile de répondre à cette question. Nous espérons que les organisations internationales ayant une présence en Asie enregistreront leurs .asia.

- Quels sont vos objectifs en termes de nombre de dépôts ?

Encore une fois, ceci est difficile à mesurer a priori. Nous avons reçu beaucoup d'email d'encouragement et beaucoup de demandes de renseignements à propos .asia. Comme vous le savez la région Asie Pacifique est très vaste et diverse. Nous espérons rencontrer le même succès que le .eu !

Mail Club mailclub.info

R.D.T.I.C
LA REVUE DU DROIT DES TECHNIQUES DE L'INFORMATION ET DE LA COMMUNICATION-
N°60 – JANVIER 2007

INFORMATIQUE ET LIBERTÉS, VIE PRIVÉE

ABC DE LA PROTECTION DES DONNÉES PERSONNELLES POUR L'ANNÉE 2006

Par M. Cédric Crépin, Juriste,
Cabinet CILEX

Nous avons souhaité établir une petite rétrospective, forcément subjective, des grands événements de cette année 2006. Le grand événement a évidemment été l'émergence des premiers CIL, Correspondants Informatiques et Libertés - sans oublier la création du Cabinet CILEX par vos serviteurs...

| A | B | C | D | E | F | G | H | I |

A comme AOL (Etats-Unis) qui a sans doute commis la plus grosse faute en matière de protection de la vie privée de l'année. La société a mis en ligne les données de recherche de 650.000 utilisateurs de ses services. Le nom des utilisateurs n'apparaissait pas - remplacés par des identifiants aléatoires - mais les données incluaient l'historique de recherche d'une période de 3 mois ainsi que les liens cliqués pour chacune des requêtes. Pourtant, des internautes et des journalistes ont réussi à identifier certaines personnes en recoupant les requêtes. Des poursuites judicaires contre AOL sont aujourd'hui engagées. Quelques semaines plus tôt, AOL avait accepté d'ouvrir ses bases au gouvernement américain... A noter que la loi US impose aux entreprises d'informer le public sur les pertes, vols... de données subis; on peut se demander quel serait le résultat d'une telle obligation en France...

En savoir plus :

Un article de la rédaction de ZDNet
Un article de Generation-NT
Le point de vue de l'association américaine Electronic Frontier Foundation
A, c'est aussi...

ACFCI (Assemblée des Chambres Françaises de Commerce et d'Industrie) qui a conclu en mai une convention de partenariat avec la CNIL pour promouvoir la nouvelle fonction de correspondant à la protection des données au sein des CCI, puis des entreprises ;
Assureurs santé dont les traitements sont l'objet d'une action commune de contrôle dans les 25 pays de l'Union sous l'impulsion du G29.

B comme Biométrie, technique globale visant à établir l'identité d'une personne en mesurant une de ses caractéristiques physiques. Travail (contrôles des accès), école (gestion de la restauration), police (fichiers d'empreintes, bases ADN), la biométrie connaît un succès que la CNIL a eu du mal à canaliser. D'abord hésitante sur le sujet, la Commission a adopté pas moins de trois autorisations uniques pour permettre l'encadrement des traitements à base de biométrie. Elle a en outre développé de nombreux axes de communications pour tenter de faire comprendre les enjeux et les dangers de cette technique. Objet de toutes les convoitises pour certains, rejet pur et simple pour d'autres, la biométrie fut au coeur des passions en 2006.

En savoir plus :

Les trois autorisations uniques adoptées par la CNIL
Un Rapport parlementaire du 4 mai 2006 rendant compte d'une audition publique sur la biométrie
Un article de la rédaction du JDN
Le Portail francophone de la biométrie
B, c'est aussi...

Banques, dont la pratique en matière de protection des données est cette année encore insuffisante (affaire SWIFT, santion à l'encontre du Crédit Lyonnais) ;
Blog, page personnelle dont le régime juridique a été discuté en 2006. Le blog est désormais dispensé de déclaration par la CNIL s'il est un simple journal personnel, mais il reste soumis aux dispositions de la loi.

C comme Correspondant à la protection des données, plus connu sous le sigle CIL. Issu de la loi d'août 2004 modifiant la loi Informatique et Libertés, son statut a été défini fin 2005. En un an, près de 600 organismes se sont dotés d'un CIL. Résultats satisfaisants pour certains, chiffres dérisoires - ou décevants ? - pour d'autres, la fonction est encore en phase de tâtonnements. Et vous, avez-vous un CIL / pensez-vous en mettre un en place en 2007 ? Quel est votre pronostic sur le nombre de CIL dans un an, fin 2007 ?

En savoir plus :

La page consacrée au CIL sur le site de la CNIL
Le Cabinet CILEX, dédié au CIL
Un article sur le site de 01Net
C, c'est aussi...

CNIL - Commission Nationale de l'Informatique et des Libertés - autorité sollicitée sur de nombreux dossiers mais dont l'action est freinée, notamment par un manque de moyens. Suite à son déménagement en 2006 pour une meilleure efficacité des services, auparavant dispersés, la CNIL atteindra-t-elle en 2007 son objectif de doubler le nombre de contrôles ? ;
CILEX - Le Cabinet CILEX a été créé en février 2006 pour être le premier prestataire de Services aux CIL.

D comme Déclaration, la formalité de base permettant d'officialiser la mise en oeuvre d'un traitement. Suite à la loi du 6 août 2004 modifiant la loi Informatique et Libertés, la Déclaration a connu de profonds bouleversements. Les cas de dispenses se multiplient (notamment avec le CIL), la simplification des démarches est au coeur du travail de la CNIL. Pourtant, de trop nombreux organismes négligent de déclarer leurs traitements, au risque de subir des sanctions très lourdes.

En savoir plus :

Le Guide pratique de la déclaration sur le site de la CNIL
Un article du Cabinet CILEX
Un article de Ratiatum
D, c'est aussi...

DMP (Dossier Médical Personnel) dont les expérimentations ont été autorisés par la CNIL en juin. La question de l'utilisation du NIR comme identifiant santé fait débat.

E comme Ethnie. Les thèmes de "discrimination positive" et de racisme ont animé le débat public en 2006. La question du comptage ethnique s'est ainsi développée en parallèle. Quand bien même la loi s'oppose à cette méthode, certaines voix demandent un assouplissement des règles (dont celle de M. Delnatte, commissaire à la CNIL, qui "regrette que le comptage ethnique, banal dans les pays anglo-saxons, soit interdit en France"). La CNIL reste ferme sur ses positions : seules certaines données peuvent être recueillies dans le cadre de la mise en place d'outils de mesure de la diversité des origines. S'agissant des données relatives aux origines raciales ou ethniques des personnes, l'absence de définition d'un référentiel national de typologies « ethno-raciales » prohibe toute étude de ce type. Des parades existent : en juillet, la CNIL a autorisé une enquête basée sur un échantillon sélectionné à partir de la consonance du nom et du prénom d'abonnés du téléphone "en raison de l'intérêt public attaché à l'étude de l'intégration en France des

descendants d'immigrés turcs et marocains". En décembre, elle lance une consultation publique afin de définir une position officielle.

En savoir plus :

La position de la CNIL sur le comptage ethnique
La CNIL lance une consultation publique
Les délibérations de la CNIL sur le dossier du CRIF (rejet d'une demande de sondage téléphonique)
L'audition parlementaire du président de la HALDE par la délégation aux droits des femmes
E, c'est aussi...

Europol, organisation européenne chargée de la lutte contre la criminalité créée en 1995, chargée de faciliter l'échange d'informations entre les États membres. A l'avenir, elle gèrera des bases de données européenne (dont ADN).

F comme Finances, celles de la CNIL étant dans le rouge. Face à une activité croissante suite aux modifications législatives, la CNIL manque de moyens humains et financiers pour remplir ses missions. Cette situation, dénoncée par le président Türk, a été résolue par le Premier Ministre qui a décidé de dégeler un budget promis en début d'année. La CNIL est toujours en "cessation de paiement" et demande une « sanctuarisation » de son budget, afin qu'il ne disparaisse pas sous le coup d'amendements parlementaires. Fragilisée, la CNIL regarde l'avenir avec doute.

En savoir plus :

Le communiqué de la CNIL :
L'appel du député Christian Paul sur son site (avec la réaction de l'un des commissaires de la CNIL en commentaires)
Un article de 01Net
F, c'est aussi...

Fichiers de police qui ont été multiplié en 2006 (FIJAIS, Fichier des crimes en série...), la CNIL rappellant constamment sa préoccupation autour de ces "casiers judiciaires parallèles" ;
FNAEG ou Fichier National Automatisé des Empreintes Génétiques. Réservé aux auteurs avérés de crimes sexuels à sa création en 1998, il a été progressivement été étendu aux auteurs de crimes graves (2001), puis à tous les délits et intractions, aux suspects et aux simples "mis en cause" en 2003. Le refus de prélèvement constitue un délit ; les premières condamnations ont eu lieu durant l'été 2006.

G comme G29, le méconnu groupe de travail européen des autorités nationales de protection de la vie privée. Le G29 travaille en partie sur les questions de transfert de données aux Etats-Unis, gros demandeur de données personnelles. Et l'année fut riche : affaire SWIFT (programme de surveillance des transactions financières par les autorités américaines), annulation de l'accord PNR (Passenger Name Records, enregistrement des passagers aériens) par la CJCE, mise en place de systèmes d'alertes éthiques au sein de certaines entreprises en application de la loi américaine Sarbanes-Oxley... Souvent négligé, le travail fourni par le G29 est pourtant primordial pour la protection des données au sein de l'Union Européenne.

En savoir plus :

Le site officiel du G29
Interview de Peter Shaar, président du G29 par la rédaction de ZDNet
La page de la CNIL consacré au PNR
G, c'est aussi...

Géolocalisation, technique de localisation par GSM utilisée par certaines sociétés pour suivre les employés, encadrée par la CNIL

La synthèse de la consultation publique organisée par le Forum des Droits sur l'Internet
Un article du Monde Informatique

| J | K | L | M | N | O | P | Q |

H comme HALDE, l'autorité administrative indépendante (AAI, comme la CNIL) chargée de lutter contre les discriminations et promouvoir l'égalité. En mai, la HALDE et la CNIL signent une convention de partenariat pour conjuguer leurs efforts. Echanges d'informations, mission de contrôle en commun... les deux AAI espèrent se promouvoir mutuellement, la compétence des deux instances étant parfois complémentaires (voir la lettre E).

En savoir plus :

Le site de la HALDE :
Le texte de la convention entre la CNIL et la HALDE
H, c'est aussi...

Hypermarchés, les mauvais élèves de l'année 2006 avec les dispositifs de contrôle de paiements par chèques mis en oeuvre sans autorisation de la CNIL, qui a décidé de procéder à des contrôles. A noter la condamnation d'un hypermarché Leclerc en décembre pour ces mêmes motifs.

I comme Identité ou plutôt les titres d'identité. Carte d'identité, passeport, visas sont tous l'objet de modifications importantes suite aux attentats du 11 septembre 2001. L'emploi d'éléments biométriques et la constitution de bases de données sont les points les plus discutés. En France, la CNIL nourrit sa réflexion s'agissant de la carte d'identité électronique en procédant à des auditions. Le passeport biométrique est quant à lui mis en circulation, pour faire face aux exigences américaines. En Allemagne, les données personnelles pourraient être mises en vente par l'État pour financer ces passeports.

En savoir plus :

La page de la CNIL sur la question des titres d'identité :

J comme Justice qui prend le relais de la CNIL pour condamner les infractions à la loi Informatique et Libertés. Depuis 1978, la CNIL dispose d'un pouvoir de dénonciation des infractions au Parquet ; les sanctions ainsi encourues ont été alourdies par la modification de la loi opérée en 2006.

En 2006, une société qui avait procédé à un sondage politique non anonyme (tout en l'ayant déclaré comme sondage simple) a été condamnée à une amende de 5000 € (avril) ; un dispositif d'écoutes téléphoniques mis en place par France Télécom pour améliorer son Support Client a été suspendu car non déclaré à la CNIL (avril) ; un P2Piste a été relaxé par le Tribunal Correctionnel de Bobigny en décembre, le traitement des adresses IP n'ayant pas été déclaré.

Enfin, la Cour de Cassation a défini en mars la notion de « collecte des données » dans une affaires de spam dénoncée par la CNIL (il est donc interdit d'aspirer des adresses e-mail sur des sites internet). Les tribunaux fondent fréquemment leurs décisions sur d'autres textes (loi Godfrain, LCEN...) ; le volet « Sanctions » de la loi Informatique et Libertés est ainsi assez sous-utilisé.

En savoir plus :
Un communiqué de la CNIL
L'arrêt du 14 mars 2006 de la Cour de Cassation (source Legalis.net)
Un article du Forum des Droits sur la condamnation de France Télécom

K comme Keylogger, dispositif permettant d'enregistrer l'activité d'un utilisateur à son insu (frappes de touches du clavier, clics souris...). Cette bonne vieille technique d'espionnage connait une nouvelle jeunesse. Ces logiciels permettent de récupérer des données sensibles comme les numéros de carte bancaires, de sécurité sociale, les identifiants de connexion, etc. Le CERTA a émis des recommandations de vigilance en décembre 2006, signe de la constante actualité de ce type de danger. En France, un réseau d'une dizaine de personnes a été arrêté en janvier pour avoir volé des codes d'accès de comptes bancaires en ligne via un keylogger.

En savoir plus :

Les recommandations du CERTA du 22 décembre 2006
Un article de la rédaction de 01Net

K, c'est aussi...
Kazakhstan : malgré nos efforts, nous n'avons pas trouvé trace d'une politique de Protection des Données Personnelles... pas plus qu'au Kirghizistan voisin, au Koweit ni au Kenya (non, le Kremlin n'est pas un pays). Et vous, avez-vous des informations ?

L comme Lieu de travail. Cybersurveillance, géolocalisation, gestion des accès et des horaires, mise en oeuvre de dispositifs d'alertes professionnelles... La frontière entre vie privée et activité professionnelle a connu de nombreuses modifications cette année. La Cour de Cassation a par exemple précisé sa jurisprudence « Nikon » en matière de communication électronique : « les dossiers et fichiers créés par un salarié grâce à l'outil informatique mis à sa disposition par son employeur pour l'exécution de son travail sont présumés, sauf si le salarié les identifie comme étant personnels, avoir un caractère professionnel de sorte que l'employeur peut y avoir accès hors sa présence » (C. Cass. 18 octobre 2006). La CNIL a fait face à la montée de la biométrie au sein des entreprises et au développement des outils de géolocalisation (en particulier via les dispositifs GSM). Afin de canaliser les dossiers, la Commission a adopté des autorisations uniques et des recommandations définissant un cadre légal de déploiement de ces technologies.

En savoir plus :
Les autorisations uniques adoptées par la CNIL
L'arrêt du 18 octobre 2006 de la Cour de Cassation (source Forum des Droits)
Un article sur le site de The Register

M comme Médecine ou Donnée Médicales. En la matière, l'année 2006 a été marquée par le dossier du DMP (Dossier Médical Personnel) et l'hébergement de données de santé. En janvier, un décret fixe la procédure d'agrément des hébergeurs de données de santé. En juin, la CNIL autorise l'expérimentation du DMP dans treize régions et dix-sept sites pilotes retenus par le Groupement d'intérêt public du dossier médical personnel (GIP-DMP). En décembre, le Conseil Constitutionnel censure 18 articles de la loi de financement de la Sécurité Sociale, dont deux relatifs au déploiement du DMP. Dans le même temps, l'expérience pilote menée par Santénergie tourne à la catastrophe,avec un arrêt du service pendant 3semaines et un audit de sécurité, lorsqu'un médecin testeur découvre un mécanisme de mots de passe digne d'un programmeur débutant... En 2007, on ne connait toujours pas le calendrier de mise en oeuvre du DMP.

L'inquiétude sur la protection de la vie privée des données médicales est également grandissante en Amérique du Nord. Les accès indus aux dossiers médicaux se multiplient (certaines personnalités se faisant soigner sous un faux nom) aux Etats-Unis. Au Canada les dossiers sont désormais indexés par un logiciel financé par la CIA. Deux situations mais une constante : le recul de la confiance des patients.

En savoir plus :
La CNIL autorise les expérimentations du dossier médical personnel
La décision du 14 décembre 2006 du Conseil Constitutionnel
Un article de Fulmedico sur la faille de sécurité chez Santénergie
Un article du New York Times concernant l'informatisation des données médicales
Un article de la presse canadienne

N comme NIR (Numéro d'Inscription au Répertoire d'identification des personnes), plus connu pour être le Numéro de Sécurité Sociale. A l'origine de la création de la CNIL et de la loi Informatique et Libertés suite à l'affaire SAFARI, le NIR est entouré de nombreuses précautions : l'utilisation d'un identifiant unique faciliterait l'interconnexion de fichiers, mais permettrait de tracer les individus dans tous les actes de la vie courante. Cette question revient pourtant régulièrement sur le devant de la scène : la CNIL a ainsi refusé en février l'utilisation du NIR par des organismes de recouvrement de créance au motif que la lutte contre la fraude ou l'homonymie n'est pas suffisante.

Seul l'intérêt général peut commander le recours au NIR ; dès lors, le gouvernement essaie d'activer ce levier dans le cadre du DMP : le NIR deviendrait ainsi l'identifiant santé unique permettant d'alimenter et de consulter le dossier médical du patient. La loi sur le financement de la Sécurité Sociale prévoyait une demande d'« avis conforme » de la CNIL sur cette question ; mais en décembre, le Conseil Constitutionnel a censuré cette disposition, estimant que seul un avis simple peut être demandé. L'utilisation du NIR est pour l'instant écartée...Par ailleurs, une vague d'opposition voit le jour : une pétition a été lancée pour appuyer la CNIL dans son refus l'utilisation du NIR.

En savoir plus :
Le rejet par la CNIL de l'utilisation du NIR sans motif d'intérêt général
L'actualité du NIS sur le blog du Dr. Fraslin de FULMEDICO

La position du GIP-DMP sur l'utilisation du NIR… et celle du Directeur des Services de Bull, acteur de l'expérimentation DMP
La pétition réclamant le rejet du NIR comme identifiant santé

N, c'est aussi…
Nomadisme, nouvelle forme de travail facilitée par le développement d'appareils portables. Le travail mobile et à distance peut toutefois faire courir des risques pour la protection des données. La perte d'un support (PC, CD-Rom, Clé USB) conjuguée à une sécurité défaillante (cryptage généralement inexistant) et aux erreurs humaines présentent un risque majeur pour la perte de données et leur réutilisation non autorisée.

O comme Ouverture de la CNIL sur ce qui l'entoure. La Commission a poursuivi ses efforts en matière de communication : nouvelles étapes du « Tour de France », mise en place d'un service « front-office » de renseignements téléphoniques, formations des premiers CIL, publication intégrale de délibérations de sanctions… La communication est un axe de travail important d'Alex Türk, Président de la Commission. Reste à poursuivre et améliorer les efforts entrepris, par exemple en publiant systématiquement les sanctions prises.

P comme Prospection politique, l'échéance des élections favorisant cette tendance. 2006 fut émaillée par l'affaire dite du « Sarko-spam » et l'envoi par milliers de courriers électroniques non sollicités. La CNIL est intervenue timidement dans le débat, en publiant une recommandation à l'intention des parties. Pourtant, cette affaire révèle l'interprétation extensive qui peut être faite de la LCEN – pour la CNIL, la loi autorise le « spam » BtoB – et le laxisme de certains vendeurs de fichiers d'adresses dans la segmentation des publics cibles. Il ne faut pas oublier que la loi Informatique et Libertés prohibe le traitement des idées politiques ou syndicales ; la violation de ce principe est constitutive d'un délit, passible de sanction pénale. C'est ce qu'a appris en avril le sondeur, dénoncé au Parquet par la CNIL, qui n'avait pas anonymisé ses questionnaires politiques.

En savoir plus :
La recommandation de la CNIL sur la constitution de fichiers dans le cadre d'activités politiques
Le compte-rendu de la table ronde organisée par la CNIL suite à l'affaire du « Sarko-spam » (source : Frédéric Couchet)

P, c'est aussi…
La Plainte déposée en Irlande par le Digital Rights Ireland contre la directive européenne 2006/24 CE sur la conservation des données (ce texte commande la rétention de données de connexion internet ou téléphoniques, filaires ou sans-fil). Le groupe reproche à la Directive de ne pas assurer une proportionnalité entre les mesures envisagées et la vie privée de millions d'individus.

Q comme la Question soulevée en novembre par la Conférence des Commissaires à la protection des données : « Vers une société de surveillance ? ». A cette occasion, les autorités européennes de protection des données se sont inquiétées de la multiplication des fichiers publics aux objectifs sécuritaires et de l'accélération technologique. Les manques d'anticipation, de concertation et de réflexion des pouvoirs publics sont vivement regrettés par les Commissaires européens. En France, la CNIL relaie cette idée en février puis en juillet, lorsqu'elle se demande si elle a été « écoutée » lors de l'adoption des lois antiterrorisme et prévention de la délinquance. En parallèle, l'association Privacy International dresse une carte des pays en fonction de leur niveau de surveillance.

En savoir plus :
Le rapport de la Conférence des Commissaires sur le thème de la société de surveillance
La CNIL a-t-elle été écoutée ?
L'étude de l'association Privacy International sur les sociétés de surveillance.

R comme Rétention de données, effectif et obligatoire en France depuis la publication du décret du 24 mars 2006 : un ensemble de données techniques sont désormais conservées par tous les opérateurs de communications électroniques, fournisseurs d'accès Internet, et opérateurs de téléphonie, mobile ou fixe. De même, "les personnes qui, au titre d'une activité professionnelle principale ou accessoire, offrent au public une connexion permettant une communication en ligne par l'intermédiaire d'un accès au réseau, y compris à titre gratuit, sont soumises au respect de ces dispositions".

Le principe de la conservation de données avait été posé par la loi sur la Sécurité Quotidienne en novembre 2001, soit quatre ans auparavant, avec un double objectif (outre les naturels impératifs de facturation des

opérateurs…). Un objectif de sécurité des réseaux a conduit à organiser un premier niveau de rétention de trois mois. D'autre part, pour permettre la recherche, la constatation et la poursuite des infractions pénales, les données sont conservées douze mois, indépendamment de leur nature.

La définition des données conservées est large et peu précise : identification de l'utilisateur et du destinataire, origine et localisation, caractéristiques techniques des équipements ainsi que la date, l'horaire et la durée de chaque communication… La CNIL n'a pas hésité à critiquer ce texte, estimant qu' "e*n se contentant d'énumérer cinq catégories générales de données* [le décret] *ne permet pas aux opérateurs de mesurer précisément l'obligation qui leur est faite de conserver certaines données en dérogation au principe général d'effacement ou d'anonymisation posé par la loi*". La Commission relève à l'occasion que son avis d'octobre 2005 sur l'avant-projet de loi anti-terrorisme n'a pas été suivi…

Le décret de mars 2006 applique également la Directive 2006/24 adoptée le 15 mars 2006. Ce texte européen s'était attiré les foudres du G29, groupe de travail des "CNIL" européennes. Dans un avis du 25 mars, le G29 soulignait que "*la décision de conserver les données de communication aux fins de la répression des infractions graves est sans précédent et elle fera date. Elle empiète sur la vie quotidienne de chacun et menace les valeurs et les libertés fondamentales érigées en principes et chères au coeur de tous les citoyens européens*." Cette directive fait d'ailleurs l'objet de contestations devant les juridictions Irlandaises (voir la lettre P). Enfin, à voir la dérive du fichier génétique, le FNAEG, à l'origine réservé lui aussi aux "infractions graves" et désormais applicable aux taggeurs et aux faucheurs d'OGM, on ne peut que s'interroger…

En savoir plus :
• La loi sur la sécurité quotidienne du 15 novembre 2001, le décret d'application du 24 mars 2006, et l'arrêté du 22 août 2006 proposant une grille tarifaire des compensations financières liées à la rétention des données
• L'avis de la CNIL du 10 octobre 2005 sur l'avant-projet de loi anti-terrorisme
• La réaction de la CNIL suite à l'adoption du décret du 24 mars 2006
• L'avis du G29 sur la directive 2006/24
• Un article du blog sur le E-commerce de Benoît Tabaka

R c'est aussi comme...

RATP, fautive d'une fuite de données personnelles cet été. Un particulier qui complétait en ligne un formulaire pour un pass Navigo a remarqué que l'URL comprenait en partie son numéro client. En modifiant ce numéro dans l'adresse, il parvint dynamiquement à consulter le formulaire des autres clients. La consultation des formulaires permettait d'accéder à la photo du demandeur, son état civil, son adresse postale, son mail et son numéro de téléphone. Ce défaut de sécurité, digne d'un débutant, est une violation patente de l'obligation de sécurité imposée par l'article 34 de la loi Informatique et Libertés, passible de lourdes peines. Un faux-pas de plus pour la RATP qui, en violation des recommandations de la CNIL, faisait payer aux possesseurs de Navigo la possibilité de circuler de façon anonymement. Cette faculté semble d'ailleurs avoir tout simplement disparu aujourd'hui.

RFID - Radio Frequency IDentification - méthode permettant de stocker et récupérer des données à distance. Elle peut fournir des données à caractère personnel de part la nature individuelle des identifiants de chacun des objets marqués. La CNIL et la Commission Européenne s'inquiètent des usages "furtifs" pouvant découler de cette technologie. Un cadre réglementaire est à l'heure actuelle en cours d'élaboration, le G29 ayant fourni un rapport éclairant sur les problèmes du RFID et les solutions possibles.

S comme les Sanctions de la CNIL délivrées en 2006. La modification de la loi Informatique et Libertés en août 2004 a doté la CNIL d'outils répressifs importants, notamment par un nouveau pouvoir de sanction pécuniaire. Par deux délibérations du 28 juin, une Etude d'huissier et la banque LCL ont eu la primeur publique de ce pouvoir d'amende. Dans le premier cas, la CNIL a voulu contrôler les pratiques de l'Etude suite à des plaintes. Le secret professionnel lui a été opposé, empêchant toute vérification. Après enquête, la CNIL a estimé que son action a été entravée et qu'aucun effort en matière de protection des données n'avait été fourni par l'étude.

Dans le second cas, la CNIL avait été saisie de plaintes émanant de clients de la banque LCL, contestant leur inscription dans les fichiers centraux de la Banque de France (FCC [chèques impayés, retraits carte bancaire] et FICP, incidents de remboursement aux Crédits des Particuliers). Or ces clients avaient payé leurs dettes. La CNIL a alors procédé à deux contrôles successifs, mais n'a pas obtenu de réponses satisfaisantes quant à la conformité de ces inscriptions à la réglementation bancaire applicable. Face à l'inertie de la banque lors des contrôles, la Commission a estimé qu'il y avait eu entrave à son action et inscription abusive dans des fichiers. Une amende de 45.000 € a été infligée, assortie de l'insertion de la délibération de la Commission dans deux quotidiens (Le Figaro et Les Echos) - cette insertion a eu lieu le 15 août, jour de faible lectorat. Si les pratiques Informatiques et Libertés sont à revoir, le Service Communication de la banque est quant à lui bien rodé.

En savoir plus :
• Les délibérations de la CNIL du 28 juin 2006 sanctionnant la banque LCL et une étude d'huissiers
• Un article de la rédaction de ZDNet

S c'est aussi comme...

Signal-Spam, plate-forme de concertation publique-privée destinée à lutter contre le spam. Le projet, lancé après l'expérience de la boîte à spam de la CNIL, a vocation a recueillir des données destinées aux autorités et aux fournisseurs d'accès. Un des leviers de cette action consiste en la posibiité pour l'internaute de transmettre ses courriers indésirables, ce qui renseignerait sur l'origine et la nature des spam. Prévue pour le dernier trimestre 2006, cette fonctionnalité est toujours dans les cartons en ce début d'année.

La Sécurité des Système d'Informations (SSI), dont l'importance sur la vie privée, l'économie et la stratégie de l'entreprise est sous-évaluée selon la Commission Européenne. Elle invite les Etats membres et les sociétés à fournir plus d'efforts en la matière. La Commission s'inquiète particulièrement de la multiplication des vols de données en Amérique du Nord, et de l'absence d'information sur ce type de dommage en Europe. C'est pourquoi elle a confié à une agence européenne, l'ENISA, le soin de dresser l'état des lieux des politiques de chacun des Etats membres. A terme, cela pourrait déboucher sur un système d'alerte et de partage des données au sein de l'Union Européenne.

T comme Terrorisme, moteur de la création de bases de données étatiques. Les attentats du 11 septembre 2001 qui ont frappé les Etat-Unis ont ouvert la porte à un corpus législatif sécuritaire; sous couvert du maintien de l'ordre et de la sécurité, de gigantesques bases de données voient le jour. En France, rétention des données de connexion, déploiement de la vidéosuveillance, extension du FNAEG (Fichier national Automatisé des Empreintes Génétiques) à un large panel de crimes et délits, ouverture des fichiers administratifs à la Police et à la Gendarmerie, accès aux données de voyage stockées par les transporteurs aériens... sont mis en oeuvre dans ce cadre.

Les exemples ne manquent pas pour illustrer les modifications apportées à la frontière entre vie privée et intérêt général. Si la légitimité des projets est rarement remise en cause, leur mise en oeuvre suscite diverses interrogations. La CNIL regrette régulièrement que ses avis et recommandations ne soient pas ou peu suivis; elle fustige également le manque de transparence et de garanties des traitements mis en oeuvre. La Commission n'a d'ailleurs pas hésité à monter au créneau pour critiquer ouvertement certains textes en 2006. Unique garde-fou face à la multiplication des fichiers, la loi antiterrorisme de janvier 2006 a en outre réduit son rôle sur les fichiers intéressant la sûreté de l'Etat, la Défense ou la Sécurité Publique.

Cette inflation législative se développe également en dehors de nos frontières: la plupart des pays renforcent leur législation. Des accords régionaux, destinés à la lutte contre le terrorisme, mettent en place de nouveaux traitements de données personnelles : accord PNR Europe-Etats-Unis (tranfert des données Passagers à l'administration US), développement du système VIS (système européen d'information sur les visas de court séjour), création du passeport biométrique européen, etc.

Notons enfin que ce développement, faisant craindre un recul global des libertés, provoque réactions et émergence de contre-pouvoirs, favorisés par l'Internet. L'association StateWatch propose ainsi d'analyser les réformes entreprises du point de vue des libertés publiques ; Privacy International a créé les célèbres Big Brother Awards ; l'Electronic Frontier Fondation, EPIC.org... alimentent tous ces polémiques. En France, citons l'IRIS, "Imaginons un Réseau Internet Solidaire".

En savoir plus :
• La page de la CNIL consacrée aux traitements relatifs à l'antiterrorisme
• L'étude menée par l'association StateWatch sur le développement des législations sécuritaires
• Un article de Wired sur la position de la FTC suite aux attentats de 2001
• Un article de synthèse de la rédaction de 01Net, fin 2005, sur les mesures antiterroristes

T c'est aussi comme...

Le Tribunal Assisté par Ordinateur (TAO) testé en Chine sur plus de mille cinq cent affaires criminelles (meurtres, cambriolage, crimes sexuels...). Concrètement, le juge renseigne certains éléments de l'affaire au logiciel (nature du crime, préjudice subi par la victime, circonstances atténuantes ou aggravantes...) qui propose une sanction. Étrangement, cette aide informatique a pour but de combattre l'arbitraire et l'abus de pouvoir de certains magistrats chinois…

U comme l'Urgence invoquée par le Président de la CNIL, Alex Türk, à communiquer auprès du grand public sur les questions de protection des données. Cette initiative, relayée par le Commissaire Européen à la Protection des Données (CEPD) - actuellement Peter Johan Hustinx - et par la Conférence des Commissaires (Londres 2006), est destinée à provoquer un réveil des consciences chez les citoyens. Une dizaine de "CNIL"

dans le monde soutiennent cette action conjointe. Procédant à une véritable remise en cause, les autorités de protection des données soulignent le discrédit dont elles sont généralement victimes : image trop juridique ou technocratique, sous-représentation médiatique, relations avec l'extérieur (société civile, associations, chercheurs) insuffisantes...

Dans un document stratégique de novembre 2006, le Président Türk propose d'établir un parallèle entre protection de l'environnement et protection de la vie privée. Dans les deux cas, la notion de capital à conserver est évoquée. Sur le plan de l'action, la rédaction d'une Charte Universelle de la Protection des Données est envisagée. L'urgence dénoncée par Alex Türk doit trouver un écho dans les actions des autorités de protection et, dans une plus large mesure, la conscience collective, pour ne pas rester un simple voeu pieux.

En savoir plus :
• Le document stratégique publié par la Conférence des Commissaires de Londres en novembre 2006
• Le site du Commissaire Européeen à la Protection des Données, Peter Johan Hustinx
• Un article de la rédaction de The Register (Londres) sur la conférence des Commissaires
• La tribune d'Alex Türk sur le site de la CNIL

U c'est aussi comme...

UMP (Union pour un Mouvement Populaire), qui a alimenté l'actualité de la protection des données en 2006. L'affaire dite du "Sarko-spam"(campagne de recrutement par e-mailing à la légalité contestée) a largement contribué à cette "notoriété". Toutefois, le parti s'est aussi distingué par une affaire de fuite de données. Un fichier Excel comprenant trois mille cinq cent noms d'adhérents ainsi que leurs données personnelles a été joint - par erreur - lors de l'envoi d'une campagne d'e-mailing.

La faute est double : d'une part, le recours à Excel ou Word pour constituer un fichier d'adhérents est un très mauvais réflexe (aucune sécurité, aucun mécanisme contrôlé de gestion...). D'autre part, l'absence de cryptage des données a permis leur reproduction sur plusieurs sites internet. Le parti a toutefois contacté la CNIL rapidement, et a envoyé un mail à ses adhérents pour signaler cette erreur et inviter à la suppression du mail litigieux. Si l'UMP a été mise sur le devant de la scène, tous les partis sont concernés. Le site zataz.com a ainsi révélé les failles de sécurité affectant les sites web des partis politiques, laissant la porte ouverte à des usages frauduleux.

V comme la Vente de la Vie pivée. La commercialisation de données à caractère personnel n'a en elle-même aucun caractère prohibé… mais elle doit respecter la loi Informatique et Libertés. Les conditions de légalité doivent être respectées : information et accord de la personne concernée, droit d'accès, de rectification et de suppression des données chez l'acheteur, accomplissement des formalités préalables par l'acheteur et/ou le vendeur auprès de la CNIL (Déclaration, voire Autorisation...)… Bien que contraignantes, ces règles garantissent la protection de la vie privée.

En Europe, la vente de données, bancaires notamment, s'organise sous le manteau, via des forums et des sites douteux. Dans un autre registre, le Parc Eurodisney s'est fait épingler pour avoir payé des agents de police afin de recueillir des éléments pouvant "aider" au recrutement d'employés. En Allemagne, les députés ont évoqué (spontanément ?) l'idée de vente de données personnelles pour financer les nouveaux passeports biométriques… et ont provoqué un scandale.

Aux Etats-Unis, la vie privée est commercialisée au même titre que toute autre marchandise; des sociétés comme USSearch ou Intelius en ont fait leur très florissante activité. Des données très sensibles sont ainsi vendues : casier judiciaire, biens immobilers, historique marital… l'idéal pour tout connaître de son voisin, de son futur employé ou de sa nourrice. La négation du droit à l'oubli inhérente à ce système, facilité par les interconnexions de fichiers, crée un risque de "marquage à vie" des individus. Sur le Vieux Continent, la Loi Informatique et Libertés poursuit l'objectif inverse.

En savoir plus :
• Les sites des sociétés USSearch et Intelius
• Un article de la rédaction de Génération NT sur Intelius
• Un article de la rédaction du Monde Informatique sur le financement du passeport en Allemagne

V c'est aussi comme...

Vote électronique, levier de l'E-démocratie, dont l'opportunité continue d'alimenter le débat. La CNIL s'intéresse au sujet depuis quelques années, avec notamment une recommandation sur la sécurité des systèmes de vote électronique en juillet 2003. En février, elle a émis un avis sur le dispositif de vote électronique pour les élections à l'assemblée des Français de l'étranger (AFE). Si la recommandation de 2003 de la CNIL est respectée, la Commission regrette qu'aucune expertise indépendante du dispositif de vote électronique ne lui ait été transmise. Un "oubli" non négligeable, la CNIL n'ayant pu apprécier le dispositif de vote électronique projeté au regard des principes généraux de protection des données à caractère personnel.

En Mai 2006, la CNIL a dressé un état des lieux du vote électronique dans le monde. La Commission relève ainsi que le vote électronique est étroitement lié à la

technique, aussi bien pour son développement (réservé aux pays à l'infrastructure avancée) que pour son refus (l'immaturité des dispositifs techniques étant en cause). Dès lors, la Commission s'interroge sur la caractère démocratique du vote à ditance : y aura-t-il toujours une indépendance du votant ? L'analyse des experts ne se substituera-t-elle pas au contrôle populaire ?

W comme Wi-Fi (Wireless Fidelity), technologie sans fil permettant de se connecter à un réseau. La CNIL a émis en août 2006 des recommandations sur l'usage du W-iFi, notamment sur ses aspects "sécurité". Transmises par ondes radio, les informations peuvent en effet être facilement captées et traitées par un tiers non autorisé, ce qui crée un risque pour la confidentialité des données. La Commission préconise des mesures simples à destination du grand public : filtrage des accès (clé WEP, adresse MAC), utilisation du système SSL (Secure Sockets Layers) pour les gestionnaires de contenu, permettant la mise en place d'un canal de communication chiffré entre deux machines.

Faisant preuve de la même pédagogie, la CNIL avait précédemment diffusé des conseils sur l'utilisation des ordinateurs portables. Le risque de perte des données stockées sur un PC portable est réel, les nombreux vols de données déclarés aux Etats-Unis en étant la preuve suffisante (voir la lettre N). La CNIL reconnaît l'insuffisance des mesures prescrites, mais le but est bien de communiquer et de faire adopter les bons réflexes Informatique et Libertés. La Commission invite d'ailleurs les entreprises, collectivités, associations à sensibiliser leurs utilisateurs au caractère confidentiel des données mises à disposition, par le biais de notes internes et formations

En savoir plus :
• Les recommandations de la CNIL sur le Wi-Fi
• Les recommandations de la CNIL sur l'usage des ordinateurs portables
… mais aussi faire une simple recherche sur internet (avec par exemple "wep, linux, crack ") pour se rendre compte que de tels outils "pour les nuls" existent pour de vrai !

W c'est aussi comme...

Les sites Web dont la déclaration a été supprimée par la CNIL en juin 2006. Sur le plan juridique, cette solution est logique puisqu'un site Web n'est pas un traitement par lui-même, mais un moyen technique de diffusion et de collecte des données. La fin abrupte de ce service et les difficultés rencontrées par la CNIL pour expliquer la marche à suivre à l'avenir ont coupé l'Autorité d'une partie de ses "adeptes", en particulier les webmasters. Dans le même temps, la CNIL franchit le pas de la dématérialisation en permettant (enfin) de remplir l'ensemble des formalités (hormis l'autorisation) par voie électronique. Ce service, initialement destiné à faciliter les démarches des Responsables de Traitements, ne fut malheureusement pas mis en avant, demeurant confidentiel. Pour contourner toutes ces difficultés, l'idéal est évidemment de nommer un Correspondant Informatique et Libertés.

X comme Monsieur ou Madame X. L'anonymisation des décisions de justice est l'un des chantiers attaqués par la CNIL depuis plusieurs années, avec un aboutissement sous l'impulsion du Président Türk. La Commission avait établi en novembre 2001 une recommandation sur la diffusion de données personnelles sur internet par les banques de données de jurisprudence. Cette mesure préconise notamment que le nom et l'adresse des parties ou des témoins au procès soient supprimés. Soulignons que la recommandation de 2001 ne s'applique pas aux recueils de jurisprudence sur support papier ; elle ne vise que les bases de données informatisées librement accessibles sur internet.

En février, la CNIL a dressé un bilan de 5 ans d'application de ce texte. "Il apparaît que les principes dégagés en 2001 sont, pour l'essentiel, appliqués par les différents acteurs et, qu'au total, la recommandation a permis d'encadrer de manière équilibrée la diffusion des décisions de justice sur internet et d'assurer le respect de la vie privée des personnes citées dans ces décisions". La CNIL a toutefois retenu les difficultés d'application de sa recommandation. Une anonymisation globalisée rendrait la recherche jurisprudentielle particulièrement ardue, certaines décisions étant connues pour leur "nom". Des dérogations peuvent dès lors être envisagées.

Cette anonymisation est à rapprocher d'une mesure de 2004, sur avis de la CNIL : les décisions de changement de nom, accordées par le Garde des Sceaux, ne sont plus publiées dans la version électronique du Journal Officiel. Paraissant traditionnellement le vendredi, ces décisions étaient très suivies par les curieux avides de savoir que M. xxxxxx avait été autorisé à porter désormais le nom de "Dubland"…

En savoir plus :
• La recommandation du 29 novembre 2001 de la CNIL
• Le bilan de la CNIL sur les cinq années d'application de la recommandation de 2001 (février 2006)

Ycomme… heu
… nous avons séché sur le Y …

Yahoo a été sage cette année, mais on leur fait confiance pour 2007 !

Vous avez une idée ? Vite, un commentaire !

Z comme le Zéro pointé adressé par la Commission Européenne aux moyens mis en oeuvre dans la plupart des Etats membres en matière de lutte contre le spam. Une communication du 15 novembre pointe du doigt l'absence de coordination public-privé au sein de nombreux Etats. Si les lois "anti-spam" existent, elles ne sont que rarement appliquées et les poursuites judiciaires peuvent se compter sur les doigts d'une seule main. Seuls deux pays tirent leur épingle du jeu : les Pays Bas et la Finlande. Dans le premier cas, il a été possible de réduire le spam de 85 % au moyen des poursuites engagées par un organisme dédié à la lutte antispam, et ce en y consacrant seulement cinq personnes à plein temps et 570000 euros d'équipement. Dans le second cas, une application stricte des mesures de filtrage imposées par la loi ont permis de faire baisser le taux de spam de 80 % à 30 % des mails échangés.

La situation française, si elle n'est pas détaillée par la Commission, n'incite pas à l'optimisme. Les poursuites judiciaires sont rarissimes, la plateforme de coopération publique-privée SignalSpam n'est pas encore opérationnelle et surtout, la France est le troisième émetteur mondial - premier européen - de spam. Pourtant, l'arsenal législatif est prêt à être appliqué. La collecte déloyale d'adresses électroniques pouvant être sanctionnée de cinq ans d'emprisonnement et 300000 € d'amende (art. 226-18 du Code pénal), l'envoi de spam pouvant être lui puni de 750 € par message irrégulièrement expédié. Les fournisseurs d'accès peuvent même priver d'accès à internet leurs clients qui auraient été identifiés comme émetteurs de spam. Les solutions existent, seule l'ambition fait défaut.

En savoir plus :
• La communication de la Commission Européenne sur la lutte contre le spam (novembre 2006)
• Les chiffres 2006 du spam retenus par la Commission Européenne (source : Sophos)
• L'état du droit en France sur la question du spam sur le site de la CNIL
• Un article de la rédaction de Generation NT

DROIT-TIC .com

R.D.T.I.C

LA REVUE DU DROIT DES TECHNIQUES DE L'INFORMATION ET DE LA COMMUNICATION-
N°60 – JANVIER 2007

DECRETS

Décret n° 2007-86 du 23 janvier 2007 relatif à l'accès à certains traitements automatisés mentionnés à l'article 9 de la loi n° 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers

Décret n° 2007-86 du 23 janvier 2007 relatif à l'accès à certains traitements automatisés mentionnés à l'article 9 de la loi n° 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers

NOR: INTD0700003D

Le Premier ministre,

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

Vu le code de l'entrée et du séjour des étrangers et du droit d'asile, notamment son article R. 611-12 ;

Vu le code de la route, notamment ses articles R. 225-4 et R. 330-2 ;

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

Vu la loi n° 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers, notamment ses articles 9, 32 et 33 ;

Vu le décret n° 2005-1726 du 30 décembre 2005 relatif aux passeports électroniques ;

Vu l'avis de la Commission nationale de l'informatique et des libertés en date du 5 octobre 2006 ;

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

Décrète :

Article 1

Après le deuxième alinéa de l'article R. 225-4 du code de la route, sont ajoutés quatre alinéas ainsi rédigés :

« Peuvent en outre accéder aux données mentionnées à l'article L. 225-4, dans les conditions fixées aux articles 9 et 33 de la loi n° 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles transfrontaliers :

- les agents des services de la direction générale de la police nationale et de la direction générale de la gendarmerie nationale chargés des missions de prévention et de répression des actes de terrorisme ;

- les agents des services de renseignement du ministère de la défense chargés des missions de prévention des actes de terrorisme.

Les dispositions prévues aux troisième, quatrième et cinquième alinéas sont applicables jusqu'au 31 décembre 2008. »

Article 2

Après le deuxième alinéa de l'article R. 330-2 du code de la route, sont ajoutés quatre alinéas ainsi rédigés :

« Peuvent également accéder aux données mentionnées à l'article L. 330-2 du code de la route dans les conditions fixées aux articles 9 et 33 de la loi n° 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles transfrontaliers :

- les agents des services de la direction générale de la police nationale et de la direction générale de la gendarmerie nationale chargés des missions de prévention et de répression des actes de terrorisme ;

- les agents des services de renseignement du ministère de la défense chargés des missions de prévention des actes de terrorisme.

Les dispositions prévues aux troisième, quatrième et cinquième alinéas sont applicables jusqu'au 31 décembre 2008. »

Article 3

L'article R. 611-12 du code de l'entrée et du séjour des étrangers et du droit d'asile est ainsi modifié :

1° Il est inséré avant le premier alinéa un « I » ;

2° L'article est ainsi complété :

« II. - Peuvent également accéder aux données enregistrées dans le traitement prévu à l'article R. 611-8 dans les conditions fixées aux articles 9 et 33 de la loi n°

2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles transfrontaliers :

- les agents des services de la direction générale de la police nationale et de la direction générale de la gendarmerie nationale chargés des missions de prévention et de répression des actes de terrorisme ;

- les agents des services de renseignement du ministère de la défense chargés des missions de prévention des actes de terrorisme.

III. - Les dispositions du II sont applicables jusqu'au 31 décembre 2008. »

Article 4

Après l'article 21 du décret du 30 décembre 2005 susvisé, est ajouté un article 21-1 ainsi rédigé :

« Art. 21-1. - Peuvent accéder aux données enregistrées dans le traitement prévu à l'article 18 dans les conditions fixées aux articles 9 et 33 de la loi n° 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles transfrontaliers :

- les agents des services de la direction générale de la police nationale et de la direction générale de la gendarmerie nationale chargés des missions de prévention et de répression des actes de terrorisme ;

- les agents des services de renseignement du ministère de la défense chargés des missions de prévention des actes de terrorisme.

Les dispositions du présent article sont applicables jusqu'au 31 décembre 2008. »

Article 5

Le ministre d'Etat, ministre de l'intérieur et de l'aménagement du territoire, la ministre de la défense et le ministre des transports, de l'équipement, du tourisme et de la mer sont chargés, chacun en ce qui le concerne, de l'exécution du présent décret, qui sera publié au Journal officiel de la République française.

Fait à Paris, le 23 janvier 2007.

.

Décret n° 2007-87 du 23 janvier 2007 relatif au système informatisé de gestion des dossiers des ressortissants étrangers en France

J.O n° 21 du 25 janvier 2007 page 1426, Texte n° 3.

Décret n° 2007-87 du 23 janvier 2007 relatif au système informatisé de gestion des dossiers des ressortissants étrangers en France et modifiant le code de l'entrée et du séjour des étrangers et du droit d'asile (partie réglementaire)

NOR: INTD0700004D

Le Premier ministre,

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

Vu le code de l'entrée et du séjour des étrangers et du droit d'asile, notamment son article D. 611-3 ;

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

Vu la loi n° 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers, notamment ses articles 9, 32 et 33 ;

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 le récépissé de la Commission nationale de l'informatique et des libertés en date du 6 octobre 2006,

Décrète :

Article 1

L'article D. 611-3 du code de l'entrée et du séjour des étrangers et du droit d'asile est ainsi modifié :

1° Il est inséré avant le premier alinéa un « I » ;

2° L'article est ainsi complété :

« II. - Peuvent en outre accéder aux données mentionnées à l'article D. 611-2, dans les conditions fixées aux articles 9 et 33 de la loi n° 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles transfrontaliers :

- les agents des services de la direction générale de la police nationale et de la direction générale de la gendarmerie nationale chargés des missions de prévention et de répression des actes de terrorisme ;

- les agents des services de renseignement du ministère de la défense chargés des missions de prévention des actes de terrorisme.

III. - Les dispositions du II sont applicables jusqu'au 31 décembre 2008. »

Article 2

Le ministre d'Etat, ministre de l'intérieur et de l'aménagement du territoire, et la ministre de la défense sont chargés, chacun en ce qui le concerne, de l'exécution du présent décret, qui sera publié au Journal officiel de la Républiquefrançaise.

Fait à Paris, le 23 janvier 2007.

DROIT-TIC .com

R.D.T.I.C

LA REVUE DU DROIT DES TECHNIQUES DE L'INFORMATION ET DE LA COMMUNICATION-N°60 – JANVIER 2007

DECISION ARCEP

Décision n° 2006-1201 du 14 décembre 2006 prise au terme de la procédure engagée à l'encontre de la société Index Multimédia

J.O n° 20 du 24 janvier 2007, texte n° 125.

Décision n° 2006-1201 du 14 décembre 2006 prise au terme de la procédure engagée à l'encontre de la société Index Multimédia (ex-123 Multimédia) en application de l'article L. 36-11 du code des postes et des communications électroniques

NOR: ARTJ0600195S

L'Autorité de régulation des communications électroniques et des postes,

Vu le code des postes et des communications électroniques, et notamment ses articles L. 32-1-II, L. 36-7, L. 36-11, L. 44 et R. 20-44-27 à R. 20-44-33 ;

Vu la décision n° 2005-0061 de l'Autorité de régulation des télécommunications, en date du 27 janvier 2005, dédiant les numéros de la forme 118XYZ pour être utilisés comme numéros d'accès aux services de renseignements téléphoniques ;

Vu la décision n° 2005-0062 de l'Autorité de régulation des télécommunications, en date du 27 janvier 2005, relative à la procédure d'attribution initiale des numéros 118XYZ ;

Vu la décision n° 2005-0063 de l'Autorité de régulation des télécommunications, en date du 27 janvier 2005, relative aux modalités de transition des services de renseignements téléphoniques entre les numéros d'anciens formats et le format 118XYZ ;

Vu le règlement intérieur de l'Autorité de régulation des télécommunications, tel que modifié par la décision n° 2006-0044 de l'Autorité en date du 10 janvier 2006, et notamment ses articles 19 à 26 ;

Vu la décision n° 2005-0576 de l'Autorité de régulation des communications électroniques et des postes en date du 23 juin 2005 attribuant des ressources en numérotation à la société 123 Multimédia (numéros 118 200 et 118 855) ;

Vu la décision du directeur général de l'Autorité de régulation des communications électroniques et des postes en date du 12 septembre 2006 portant mise en demeure de la société Index Multimédia de se conformer aux dispositions de l'article 4 de la décision n° 2005-0576 du 23 juin 2005 ;

Vu la décision n° 2006-1049 de l'Autorité en date du 12 octobre 2006 abrogeant l'attribution de ressources en numérotation à la société Index Multimédia (numéro 118 855) ;

Vu le courrier du directeur général de l'Autorité en date du 12 juin 2006 adressé à la société Index Multimédia lui demandant d'indiquer quelle utilisation est faite des ressources en numéros attribuées au titre de la décision n° 2005-0576 en date du 23 juin 2005 susvisée ;

Vu le courrier de l'adjoint au chef du service juridique de l'Autorité en date du 17 juillet 2006 adressé à la société Index Multimédia l'informant de l'ouverture d'une procédure de sanction en application de l'article L. 36-11 du code des postes et des communications électroniques, et portant nomination des rapporteurs ;

Vu le courrier des rapporteurs en date du 19 juillet 2006 adressé à la société Index Multimédia lui transmettant un questionnaire et fixant au 18 août 2006 la clôture du délai de réponse ;

Vu les observations de la société Index Multimédia enregistrées le 6 octobre 2006 en réponse à la mise en demeure susvisée ;

Vu le courrier de l'adjoint au chef du service juridique en date du 19 octobre 2006 notifiant à la société Index Multimédia le rapport exposant les faits et griefs retenus établi par les rapporteurs et l'invitant à consulter le dossier ;

Vu le courrier de l'adjoint au chef du service juridique en date du 6 novembre 2006 convoquant la société Index Multimédia à une audience devant le collège le jeudi 23 novembre 2006 ;

Vu le courrier électronique en date du 16 novembre 2006 de la société Index Multimédia indiquant son représentant à l'audience du 23 novembre 2006 ;

Après avoir entendu, le 23 novembre 2006, lors de l'audience devant le collège, (composé de M. Paul Champsaur, président, Mme Joëlle Toledano, MM. Edouard Bridoux, Nicolas Curien, Michel Feneyrol) :

- le rapport de M. Bertrand Pailhès, rapporteur,

- les observations de M. Philippe Pisani, directeur

général adjoint de la société Index Multimédia ;

En présence de :

- Philippe Distler, directeur général, François Lions, directeur général adjoint, M. Bertrand Pailhès, Mmes Leyla Mérini, Joëlle Adda, Christine Galliard ;

Le collège en ayant délibéré le 14 décembre 2006, hors la présence des rapporteurs et des agents de l'Autorité,

1. Dispositions légales et réglementaires

En application de l'article L. 32-1-II du code des postes et des communications électroniques susvisé, il est dans les attributions de l'Autorité de régulation des communications électroniques et des postes de prendre, « (...) dans des conditions objectives et transparentes, des mesures raisonnables et proportionnées aux objectifs poursuivis (...) » et de veiller « 11) A l'utilisation et à la gestion efficaces (...) des ressources de numérotation ; (...) ».

En vertu des dispositions de l'article L. 36-7 (7°), l'Autorité est tenue de veiller à la bonne utilisation des ressources en numérotation. Elle attribue ces ressources aux opérateurs en fonction des besoins de leur activité et dans les conditions prévues par l'article L. 44 du code des postes et des communications électroniques.

L'article L. 44 du code des postes et des communications électroniques précise que : « L'Autorité attribue, dans des conditions objectives, transparentes et non discriminatoires, aux opérateurs qui le demandent, des préfixes et des numéros ou blocs de numéros, moyennant une redevance fixée par décret en Conseil d'Etat, destinée à couvrir les coûts de gestion du plan de numérotation téléphonique et le contrôle de son utilisation.

La décision d'attribution précise les conditions d'utilisation de ces préfixes, numéros ou blocs de numéros qui portent sur :

a) Le type de service auquel l'utilisation des ressources attribuées est réservée ;

b) Les prescriptions nécessaires pour assurer une bonne utilisation des ressources attribuées ;

(...) ».

Par la décision n° 2005-0576 susvisée, l'Autorité de régulation des communications électroniques et des postes a attribué, le 23 juin 2005, des ressources en numérotation (les numéros 118 200 et 118 855) à la société Index Multimédia (anciennement 123 Multimédia) en vue de l'ouverture de services de renseignements téléphoniques.

L'article 4 de cette décision d'attribution dispose expressément que : « Tout numéro attribué à l'article 1er doit faire l'objet d'une utilisation dans les douze mois à compter de la date d'attribution. Si aucune ouverture commerciale de service de renseignements, n'a lieu dans le délai imparti, l'Autorité de régulation des communications électroniques et des postes pourra retirer le numéro sans autre préavis. Cette mesure n'exclut pas, le cas échéant, la mise en oeuvre de la procédure de sanction prévue par l'article L. 36-11 du code des postes et des communications électroniques ».

2. Exposé des faits

Par un courrier en date du 17 juillet 2006, l'adjoint au chef du service juridique de l'Autorité a informé la société Index Multimédia de l'ouverture d'une procédure de sanction relative au respect des prescriptions définies dans l'article 4 de la décision n° 2005-0576 de l'Autorité en date du 23 juin 2005 précitée.

Dans le cadre de l'instruction du dossier, les rapporteurs ont constaté que la société Index Multimédia n'avait pas respecté les dispositions relatives à l'ouverture d'un service de renseignements téléphoniques. Dans ces conditions, le directeur général de l'Autorité l'a mise en demeure, par décision en date du 12 septembre 2006, de justifier, dans un délai d'un mois, de la mise en oeuvre des mesures prises en vue d'assurer le respect des dispositions relatives aux obligations d'ouverture d'un service de renseignements.

La société Index Multimédia a répondu par courrier enregistré par les services de l'Autorité le 6 octobre 2006.

3. Réponse de la société Index Multimédia à la mise en demeure

En réponse à la décision de mise en demeure susvisée, la société Index Multimédia a, par courrier reçu le 6 octobre 2006, fait valoir les observations suivantes :

En premier lieu, elle rappelle qu'elle a adressé le 29 septembre 2006 un courrier recommandé à l'Autorité expliquant qu'elle n'était pas en mesure d'exploiter

commercialement le numéro 118 855 et qu'elle souhaitait par conséquent remettre à disposition ledit numéro.

En deuxième lieu, et concernant le numéro 118 200, la société Index Multimédia indique qu'elle n'avait pas, pour l'heure, trouvé de modèle économique adapté, qu'elle procédait à une veille du marché afin de déterminer un tarif utilisateur uniforme, et qu'elle étudiait avec attention la possibilité d'offrir un portail multiservices élargissant de fait la gamme des services offerts aux clients finaux.

4. Eléments présentés lors de l'audience du 23 novembre 2006

Le représentant de la société index Multimédia, lors de l'audience du 23 novembre 2006, a présenté la situation de la société en question.

A titre liminaire, il indique que la ressource en numérotation 118 200 n'est pas exploitée. Il confirme également que la société Index Multimédia n'a pas respecté l'article 4 de la décision n° 2005-0576 de l'Autorité du 23 juin 2005.

En outre, il indique que, compte tenu de nombreux changements de direction en un an, la société Index Multimédia n'a pu répondre au questionnaire des rapporteurs.

Sur la mise en oeuvre des services de renseignements, il souligne que la société Index Multimédia avait étudié deux options. La première option finalement abandonnée ne reposait que sur l'« annuaire universel » tandis que la seconde option tendait à rechercher des services à valeur ajoutée offerts en complément.

La première option s'étant heurtée à un problème de promotion, c'est la seconde option qui a donc été privilégiée par la société Index Multimédia qui en étudie la mise en oeuvre depuis plusieurs mois.

A cette fin, le représentant de la société Index Multimédia précise en audience que la société Index Multimédia est en négociation avec un prestataire.

Sur la question relative au calendrier prévisionnel, il indique que le plan d'affaires de cette société devrait être défini à la mi-décembre, ce qui devrait permettre le lancement de leurs services, normalement pour le début de l'année 2007.

D'un point de vue financier, il précise que 10 % du budget publicitaire annuel de la société index Multimédia auraient dû être affectés à ce projet sur le 118 200, ce qui ne fut pas le cas cette année car aucun investissement n'a finalement été fait sur ce projet, le numéro n'ayant pas été lancé. Il estime que, d'ici à la mi-décembre, la société Index Multimédia aura une estimation de l'investissement publicitaire qui pourra être consacré au numéro 118 200.

Le représentant de la société Index Multimédia indique que la société a quasiment finalisé ses contrats concernant les aspects techniques (centres d'appels, base de données de l'annuaire universel, etc.).

Aucun élément écrit n'a été apporté par le représentant de la société Index Multimédia à l'appui de ses allégations.

5. Analyse de l'Autorité des réponses apportées

par la société Index Multimédia

L'article 4 de la décision n° 2005-0576 de l'Autorité en date du 23 juin 2005 prévoit que : « Tout numéro attribué à l'article 1er doit faire l'objet d'une utilisation dans les douze mois à compter de la date d'attribution. Si aucune ouverture commerciale de service de renseignement n'a lieu dans le délai imparti, l'Autorité de régulation des communications électroniques et des postes pourra retirer le numéro sans autre préavis. Cette mesure n'exclut pas, le cas échéant, la mise en oeuvre de la procédure de sanction prévue par l'article L. 36-11 du code des postes et des communications électroniques. »

Pour rappel, les rapporteurs n'ont reçu aucune réponse écrite de la société Index Multimédia à leur questionnaire du 19 juillet 2006.

L'Autorité constate que la société Index Multimédia n'a fourni aucun élément probant et circonstancié en vue d'une ouverture effective d'un service de renseignement sur les numéros 118 200 et 118 855 et n'a justifié de la mise en oeuvre d'aucune mesure en ce sens.

En outre, l'Autorité relève que ce n'est qu'à la suite de la mise en demeure du directeur général en date du 12 septembre 2006 que la société Index Multimédia s'est exprimée en informant l'Autorité qu'elle restituait le numéro 118 855.

Concernant le numéro 118 200, la société Index Multimédia a précisé qu'elle procédait à « une veille du marché afin de déterminer un tarif utilisateur uniforme » tout en étudiant « avec attention la possibilité d'offrir un portail multiservices élargissant de fait la gamme des services offerts aux clients finaux ».

Toutefois, l'Autorité constate que la réponse de la société Index Multimédia sur l'utilisation du numéro 118 200 se borne à des affirmations qui ne sont étayées par aucun élément tangible. En outre, elle n'apporte aucun élément

suffisamment probant et circonstancié aux questions qui lui avaient été posées dans le cadre de l'instruction notamment dans le questionnaire des rapporteurs.

Il ressort de l'exposé des faits et des observations de la société Index Multimédia que celle-ci n'a apporté aucune information précise concernant notamment d'éventuelles mesures concrètes prises depuis un an pour mettre en service sur le numéro 118 200, un service universel de renseignement téléphonique, de même qu'elle n'a produit aucun calendrier prévisionnel précis de l'ouverture commerciale d'un tel service. En outre, lors de l'audience en date du 23 novembre 2006, la société Index Multimédia n'a pas contesté ces faits.

Il apparaît également qu'aucun investissement financier n'a pour le moment été réalisé par la société Index Multimédia pour la mise en oeuvre d'un service universel de renseignement téléphonique, sur la ressource en numérotation 118 200.

Enfin, la description de ses projets concernant le numéro 118 200 reste très imprécis comparativement aux services autorisés sur ce type de numéros, les options présentées par le représentant de la société Index Multimédia n'étant pas étayées par des éléments suffisamment précis concernant l'exploitation technique de l'activité envisagée.

L'Autorité constate que la société Index Multimédia ne produit aucun élément probant permettant d'attester la crédibilité d'une ouverture prochaine d'un service universel de renseignements téléphoniques accessible par le numéro 118 200 par la société Index Multimédia.

Dans ces conditions, l'Autorité considère que la société Index Multimédia n'a pas mis en oeuvre les mesures de nature à permettre le respect des dispositions de l'article 4 de la décision n° 2005-0576 susvisée de l'Autorité en date du 23 juin 2005.

6. Conclusion

1. Il y a lieu de sanctionner la société Index Multimédia au vu des faits et motifs exposés ci-dessus.

L'Autorité estime, au vu des faits et motifs exposés ci-avant, qu'il y a lieu de sanctionner la société pour le non-respect des dispositions relatives à l'ouverture d'un service de renseignements téléphoniques prévues à l'article 4 de la décision n° 2005-0576 susvisée de l'Autorité en date du 23 juin 2005.

2. Sur la nature de la sanction :

Aux termes de l'article L. 36-11 (2°) du code des postes et des communications électroniques, « lorsqu'un exploitant de réseau ou un fournisseur de services ne se conforme pas (...) à la mise en demeure prévue au 1° ci-dessus, l'Autorité de régulation des communications électroniques peut prononcer à son encontre une des sanctions suivantes :

(...)

b) Soit, en fonction de la gravité du manquement : la suspension totale ou partielle, pour un mois au plus, la réduction de la durée, dans la limite d'une année, ou le retrait de la décision d'attribution ou d'assignation prise en application des articles L. 42-1 ou L. 44. (...) »

En l'espèce, l'Autorité constate la gravité du manquement reproché à la société Index Multimédia découlant de la non-ouverture de son service de renseignements téléphoniques.

De plus, l'Autorité considère que la société Index Multimédia n'a pas mis en oeuvre de mesures de nature à permettre le respect des dispositions relatives à l'ouverture d'un service de renseignements téléphoniques prévues à l'article 4 de la décision n° 2005-0576 susvisée de l'Autorité en date du 23 juin 2005.

En fonction de ces éléments, l'Autorité estime qu'il y a lieu, compte tenu du degré de gravité du manquement constaté, de retirer l'autorisation attribuant à la société Index Multimédia la ressource en numérotation 118 200,

Décide :

Article 1

L'Autorité prononce le retrait de la décision n° 2005-0576 de l'Autorité de régulation des communications électroniques et des postes en date du 23 juin 2005 en tant qu'elle attribue à la société 123 Multimédia (nouvellement dénommée Index Multimedia) la ressource en numérotation 118 200.

Article 2

La présente décision prend effet à compter de sa notification.

Article 3

Le chef du service juridique de l'Autorité ou son adjoint est chargé de la notification de la présente décision à la société Index Multimédia. Elle sera publiée au Journal officiel de la République française.

Fait à Paris, le 14 décembre 2006.

Décision n° 2006-1173 du 5 décembre 2006 relative au questionnaire pour la collecte d'informations nécessaires au suivi des marchés mobiles

J.O n° 7 du 9 janvier 2007, texte n° 66

Autorité de régulation des communications électroniques et des postes

Décision n° 2006-1173 du 5 décembre 2006 relative au questionnaire pour la collecte d'informations nécessaires au suivi des marchés mobiles

NOR: ARTT0600184S

L'Autorité de régulation des communications électroniques et des postes,

Vu la directive n° 2002/19/CE du Parlement européen et du Conseil du 7 mars 2002 relative à l'accès aux réseaux de communications électroniques et aux ressources associées, ainsi qu'à leur interconnexion (directive « accès ») ;

Vu la directive n° 2002/20/CE du Parlement européen et du Conseil du 7 mars 2002 relative à l'autorisation de réseaux et de services de communications électroniques (directive « autorisation ») ;

Vu la directive n° 2002/21/CE du Parlement européen et du Conseil du 7 mars 2002 relative à un cadre réglementaire commun pour les réseaux et services de communications électroniques (directive « cadre ») ;

Vu la directive n° 2002/22/CE du Parlement européen et du Conseil du 7 mars 2002 concernant le service universel et les droits des utilisateurs des réseaux et services de communications électroniques (directive « service universel ») ;

Vu le code des postes et des communications électroniques, notamment ses articles L. 32-1, L. 32-4, L. 37-1, D. 98-11 et D. 98-12 ;

Après avoir délibéré le 5 décembre 2006 :

L'Autorité met en place un dispositif de recueil trimestriel d'informations auprès des opérateurs mobiles (opérateurs de réseau et opérateurs virtuels) et portant sur des éléments quantitatifs et qualitatifs relatifs à leur activité, aux fins de suivi du marché.

I. - Le cadre juridique applicable

Le pouvoir général d'information

En vertu de l'article L. 32-4 code des postes et des communications électroniques (CPCE), l'Autorité dispose d'un pouvoir général d'information lui permettant de recueillir auprès des personnes physiques ou morales exploitant des réseaux de télécommunications ou fournissant des services de télécommunications les informations ou documents nécessaires pour s'assurer du respect par ces personnes des principes définis aux articles L. 32-1 et L. 32-3, ainsi que les obligations qui leur sont imposées au titre du CPCE.

L'article L. 32-1 (II) dispose que l'ARCEP veille notamment :

« 2° A l'exercice au bénéfice des utilisateurs d'une concurrence effective et loyale entre les exploitants de réseau et les fournisseurs de services de communications électroniques ;

3° Au développement de l'emploi, de l'investissement efficace dans les infrastructures, de l'innovation et de la compétitivité dans le secteur des communications électroniques ;

4° A la définition de conditions d'accès aux réseaux ouverts au public et d'interconnexion de ces réseaux qui garantissent la possibilité pour tous les utilisateurs de communiquer librement et l'égalité des conditions de la concurrence ;

(...)

10° A la mise en place et au développement de réseaux et de services et à l'interopérabilité des services au niveau européen ;

11° A l'utilisation et à la gestion efficaces des fréquences radioélectriques et des ressources de numérotation ».

L'analyse des marchés

En vertu de l'article L. 37-1 du CPCE, l'Autorité doit déterminer les marchés du secteur des communications

électroniques pertinents en vue de l'application des articles L. 38 à L. 38-2. Elle doit ensuite, après avoir analysé l'état et l'évolution prévisible de la concurrence sur ces marchés, établir la liste des opérateurs réputés exercer une influence significative sur chacun de ces marchés. Enfin, il lui incombe de fixer les obligations applicables à ces opérateurs.

Il convient donc que l'Autorité dispose des éléments nécessaires à la mise en oeuvre des dispositions relatives à l'analyse des marchés. Il en résulte que les opérateurs sont tenus de fournir à l'Autorité les informations relatives à leur activité d'exploitation et d'établissement de réseaux ouverts au public ou de fourniture de services de communications électroniques au public, nécessaires pour apprécier et analyser rapidement la situation des marchés concernés et leurs évolutions au cours du temps.

Règles portant sur l'information des utilisateurs

En outre, en vertu du I de l'article D. 98-12, les exploitants de réseaux ouverts au public et fournisseurs de services de communications électroniques au public communiquent à l'ARCEP, sur sa demande, outre les informations prévues aux articles L. 111-1 et, le cas échéant, L. 121-18 du code de la consommation, des informations sur :

« - les conditions générales et contractuelles de fourniture du service fourni dans le cadre de sa déclaration, qui précisent :

- les conditions de renouvellement des contrats ainsi que, le cas échéant, toute durée contractuelle minimale ;

- les conditions relatives à la qualité de service ;

- les délais de fourniture et les types de services de maintenance offerts ;

- s'agissant du service téléphonique au public, la description des services offerts dans le cadre des contrats proposés ;

- les tarifs de ses offres, y compris les formules de réductions tarifaires ;

- les formules d'indemnisation et de remboursement proposées, ainsi que les mécanismes de règlement des litiges. »

II. - Les objectifs poursuivis par l'Autorité

Par sa décision n° 2005-0321, en date du 14 juin 2005, l'Autorité a mis en place un questionnaire visant la collecte d'informations nécessaires à l'application de l'article L. 37-1 du CPCE. Ce recueil annuel d'informations quantitatives permet à l'Autorité de tenir à jour les données sur lesquelles peuvent être fondées ses analyses de marchés pour en observer les évolutions et, le cas échéant, être en mesure de réexaminer la situation des marchés pertinents si les évolutions observées le justifient.

S'agissant plus spécifiquement du marché mobile, un recueil d'informations spécifique a été institué dans le cadre de l'Observatoire des mobiles. Eu égard aux évolutions régulières et fréquentes de ce marché et de son importance dans le secteur de communications électroniques, cette publication, en temps quasi réel, s'est faite sur une base initialement mensuelle puis désormais trimestrielle.

Par ailleurs, le marché de gros de l'accès et de départ d'appel mobile, marché n° 15 de la recommandation de la Commission européenne, a fait l'objet d'une analyse de marché formelle de l'Autorité. L'analyse, qui concluait à l'imposition d'un remède prenant la forme d'une obligation d'accès en métropole et d'une obligation d'itinérance de déploiement dans la zone Antilles-Guyane, a été suspendue en vue de prendre la pleine mesure de l'impact de l'apparition récente d'opérateurs virtuels sur l'animation du marché de détail en métropole. Ainsi, les marchés de gros et de détail de l'accès et du départ d'appel mobile ont été mis sous surveillance, dans l'attente de la notification d'une nouvelle analyse à la Commission en 2006.

Enfin, les nouveaux services constituent un enjeu majeur en termes d'animation du marché à moyen terme, ce qui justifie d'en suivre le développement.

Les éléments développés ci-dessus justifient un suivi spécifique des marchés mobiles, selon une fréquence trimestrielle, au travers d'un recueil d'informations alimentant les documents de restitution décrits au VI de la présente décision, par le biais du questionnaire annexé à la présente décision. Dans ce cadre il convient également que les opérateurs transmettent systématiquement les évolutions principales de leurs offres conformément au I de l'article D. 98-12 du CPCE.

III. - Les sociétés concernées par le suivi des marchés mobiles

Devront répondre au recueil d'informations trimestriel tous les opérateurs mobiles, qu'il s'agisse de sociétés exploitant ou établissant un réseau de communications électroniques ouvert au public (opérateurs de réseau) ou

fournissant au public un service de communications électroniques (opérateurs virtuels).

Les opérateurs concernés à la date de la présente décision sont les suivants :

- pour la métropole : Orange France, SFR, Bouygues Telecom, Transatel, Debitel, Omer Télécom, Futur Télécom, NRJ mobile, Neuf Cegetel, Tele2, Ten, Auchan Télécom, Carrefour Hypermarché SAS, Mobisud et Coriolis Télécom ;

- pour la zone Antilles-Guyane : Orange Caraïbe, Digicel AFG, Outremer Télécom, Dauphin Télécom, Saint-Martin Mobile, Saint-Martin et Saint-Barthélemy Tel Cell, Oceanic Digital FWI ;

- pour la Réunion : Orange Réunion, SRR, Outremer Télécom ;

- pour Mayotte : SRR, Outremer Télécom ;

- pour Saint-Pierre-et-Miquelon : SAS SPM.

IV. - La nature des éléments collectés

Le recueil d'informations est formalisé par un questionnaire annexé à la présente décision, qui sera renseigné sur une base trimestrielle par les opérateurs. Le champ des informations demandées prend en compte les spécificités des territoires considérés ainsi que la nature des acteurs (opérateurs de réseau ou opérateur virtuel), voire leur dimension.

Les informations demandées portent le cas échéant sur différents segments de clientèle, notamment la clientèle entreprises et, au sein du grand public, les clients prépayés et postpayés.

Elles permettent notamment à l'Autorité d'apprécier :

- la dimension du marché, notamment en termes de parc de clients, y compris à un niveau régional ou départemental selon le cas, ainsi que son évolution, par exemple en termes de ventes brutes et de migrations ;

- la fluidité du marché, notamment en termes de portabilité, de résiliations et d'engagement des clients ;

- le volume d'activité (chiffres d'affaires, volumes de trafic, etc.) et la dimension commerciale (offres de détail et conditions contractuelles, distribution, etc.) du marché ;

- les niveaux de prix, au-delà des tarifs faciaux des offres de détail, selon un degré de détail permettant un confort statistique suffisant ;

- le développement du marché de gros de l'accès et du départ d'appel mobile, notamment du point de vue des contrats MVNO et de leurs documents de mise en oeuvre, ainsi qu'en termes de volume d'activité (chiffres d'affaires, volumes de trafic, etc.) ;

- le développement des nouveaux services et plus généralement des technologies, y compris en termes de déploiement des équipements de réseau.

Ces informations sont proportionnées aux besoins de l'Autorité compte tenu des objectifs mentionnés au II. La liste dressée ci-dessus est non exhaustive et susceptible de donner lieu à de nouvelles évolutions, compte tenu du développement des marchés de gros et de détail.

V. - La concertation entreprise

Les premières étapes de définition du questionnaire ont été conduites en concertation avec les opérateurs. Notamment, une première réunion multilatérale a eu lieu le 7 juillet 2005, puis suivie de deux appels à commentaires des 21 septembre et 7 décembre 2005, sur des points résultant de réunions bilatérales avec des opérateurs de réseau et des opérateurs virtuels. Les opérateurs seront également associés dans les évolutions à venir du questionnaire.

VI. - Le traitement et l'utilisation des éléments collectés

Les informations recueillies par le biais du questionnaire annexé à la présente décision seront utilisées dans le cadre des objectifs fixés en II.

Ces informations feront l'objet d'une diffusion contrôlée au sein de l'Autorité et seront utilisées par le service régulation des marchés fixe et mobile, le service économie et prospective ainsi que le service opérateurs et régulation des ressources rares.

Elles permettront en particulier l'élaboration de tableaux de bord à usage interne, notamment dans le cadre de l'analyse du marché de gros de l'accès et du départ d'appel mobile. Conformément à l'article D. 295 du CPCE, une synthèse de ces tableaux de bord pourra par ailleurs être communiquée à la Commission européenne.

Enfin, sous réserve du respect du secret des affaires, elles pourront notamment être utilisées dans le cadre :

- du Suivi des indicateurs mobiles (SIM), publication trimestrielle remplaçant l'Observatoire des mobiles ;

- du rapport annuel de l'Autorité ;

- de documents soumis à consultation publique,

Décide :

Article 1

Les opérateurs mobiles exploitants de réseau et/ou fournisseurs de services concernés fournissent les éléments de réponse au questionnaire annexé à la présente décision sur un rythme trimestriel, selon le calendrier établi par le directeur général de l'Autorité.

Article 2

Le directeur général de l'Autorité est chargé de l'exécution de la présente décision, qui, à l'exception de ses annexes, sera publiée au Journal officiel de la République française.

Fait à Paris, le 5 décembre 2006.

Le président,

P. Champsaur

.