« INFORMATIQUE & LIBERTES »

DEMAIN :

QUELLES PROTECTIONS FACE A QUELLES MENACES ?

Mardi 9 avril 2002

Chambre de Commerce et d'Industrie de Paris
(Paris VIII^{ème})

En partenariat avec

Auteur : Julien Le Clainche
julien@droit-ntic.com

ACCUEIL 2
INTRODUCTION 3
LA REFONTE DU REGIME DE DECLARATION A LA CNIL 5
QUELLES NOUVELLES CONTRAINTES POUR L'ENTREPRISE ? 8
QUEL CONTROLE DE L'ETAT ? 11
SERVICES ELECTRONIQUES DE LA VILLE ET PROTECTION DU CYBER-CITOYEN 15
LA CYBERSURVEILLANCE DES SALARIES 16
MARKETING, BASES DONNEES ET VIE PRIVEE 19
GROUPES DE SOCIETE ET FLUX TRANSFRONTIERES DE DONNEES 21
SYNTHESE ET CONSLUSION 22

9h00 – 9h10

ACCUEIL

Par Frédéric Brunet, délégué du président de la Chambre de commerce et d'industrie de Paris (CCIP) pour les nouvelles technologies de l'information et de la communication (NTIC).

La France est historiquement parmi les pays pionniers de l'informatisation. Elle a su évoluer selon des modèles originaux, tels que le minitel. A ce titre, elle fut sensibilisée très tôt à la menace pour la vie privée que pouvaient représenter les évolutions techniques. C'est pourquoi la loi « Informatique et libertés » du 6 janvier 1978[1] fut adoptée.

Depuis, si la directive communautaire 95/46[2] s'est inspirée de la loi française, sa transposition nécessite des adaptations ponctuelles du texte national. La transposition aurait du intervenir au plus tard le 24 octobre 1998.

Le retard de la France à transposer la directive s'explique par la nécessité d'une réforme profonde de la loi de 1978 à la lumière des évolutions constatées ces vingt dernières années. En effet, le développement des techniques de marketing, la collecte des données à l'insu des personnes et le détournement de finalité sont des facteurs devant être pris en compte dans le cadre de la modification de la loi afin de garantir la sécurité des données et une protection efficace des droits des personnes.

Pour étroite que puisse sembler l'approche européenne dans le contexte mondial de l'Internet, un rapprochement des ordres juridiques du « vieux contient » est indispensable pour lutter contre les agissements prohibés.

A cet égard, la CCIP a publié un rapport[3] intitulé « *Transposition de la directive sur la protection des données personnelles face aux nouvelles technologies : Les conséquences pour les entreprises – Position de la CCIP*». En outre, elle a introduit dans son contrat type de commerce électronique[4] une clause spécifique à la protection des données personnelles.

[1] Loi n° 78/17 du 06 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.
[2] Directive 95/46 CE du Parlement européen et du Conseil, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à circulation de ces données.
[3] Rapport du 25 mai 2001, par J.P Saillard disponible sur le site de la CCIP.
[4] Contrat type disponible sur le site de la CCIP.

9h10 – 9h30

INTRODUCTION

Les grands changements de la prochaine loi.
Par Gérard Gouzes, député du Lot-et-Garonne, rapporteur de réforme de la loi « Informatique et libertés » du 30 novembre 2001.

En 1974, Philippe Boucher publiait un article *« SAFARI ou la chasse aux français »* qui dénonçait la menace que pouvaient constituer les traitements de données personnelles effectués par l'Etat. Cette préoccupation, est à l'origine de la loi Informatique et libertés de 1978 et du Privacy Act américain de 1974.

Ainsi, la France s'est dotée d'une autorité administrative indépendante, la Commission nationale de l'informatique et des libertés (CNIL), dont les missions sont spécifiquement dédiées à la protection des libertés au regard de la menace constituée par les fichiers de données personnelles. Il s'agit essentiellement de veiller au respect de la loi Informatique et libertés.

La CNIL a notamment :

- Une mission d'information ;
- Une mission de contrôle ;
- Un pouvoir réglementaire ;
- Un pouvoir d'investigation dont les modalités sont précisées à l'article 10 de la loi ;

Force est de constater que le développement de la micro-informatique a opéré un glissement de la menace vers le secteur privé.

La démocratisation de l'accès aux réseaux, essentiellement Internet, a considérablement accru le volume des échanges de données, notamment personnelles. Désormais, de nouvelles possibilités de traitements sont techniquement possibles et de nouveaux besoins en information sont apparus. Les traitements de données personnelles sont devenus plus que jamais un enjeu important pour les entreprises pour offrir des services nouveaux ou de meilleure qualité à leurs clients.

Ainsi, le traitement des données personnelles se pose aujourd'hui en terme de marché et les entreprises font référence aux principes du « droit marchand » :

- Liberté d'entreprendre ;
- Liberté de circulation ;
- Libre concurrence.

Une conciliation de ces principes doit être opérée avec ceux relatifs à la protection des droits des personnes. Le déplacement des risques, pris en compte dans la directive 95/46 et dans la convention 108 du Conseil de l'Europe[5], doit désormais être intégré dans la modification de la loi de 1978. Dans son rapport au Premier ministre[6], Guy Braibant estimait que la protection des droits des personnes était la contrepartie de la liberté de circulation.

[5] Convention du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE N° 108) -- disponible en ligne --
[6] « Données personnelles et société de l'information » Guy Braibant, La Documentation française, coll : rapports officiels.

Dans ce contexte, Gérard Gouzes appelle à la vigilance, notamment quant à l'utilisation NIR[7], et rappelle le débat tumultueux autour de la création de la carte vitale. Il insiste sur les aspects particuliers de l'Internet notamment, la mise en exergue du « moi social » qui incite à dévoiler sa vie privée sans se soucier des traces laissées et de leur exploitation potentielle.

Le danger réside alors dans l'existence d'un rapport de force entre l'entreprise et l'individu, à cet égard Gérard Gouzes évoque :

- L'affaire « Doubleclick » : lire l'article de Transfert, de Droit-ntic
- La cybersurveillance du salarié : voir intervention de 14h15 à 15h15.
- La sécurité de l'Etat : Lire l'article de Droit-ntic
- La santé.

Le député expose alors l'état de la transposition de la directive 95/46 dans l'ordre juridique français.

La transposition aurait dû intervenir au plus tard le 24 octobre 1998[8]. En 1996 le gouvernement avait examiné un rapport, mais celui-ci ne sembla pas donner satisfaction. En outre, la dissolution de l'Assemblée nationale en 1997 acheva de retarder le processus d'intégration de la directive en droit français. C'est finalement le rapport « Données personnelles et société de l'information » de Guy Braibant, établit en concertation avec la CNIL, qui servira de base de réflexion.

Les principes fondamentaux de la loi Informatique et libertés demeurent : « *l'informatique doit être au service de chaque citoyen. Son développement doit s'opérer dans le cadre de la coopération internationale. Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques.* »

Le projet de loi se propose de donner une définition plus claire des données à caractère personnel, comprenant notamment l'image ou la voix de la personne. De renforcer le droit à l'information et les pouvoirs de la CNIL (Contrôle a posteriori et pouvoir de sanction, pouvoir de négocier des règles déontologiques…)

Le projet de loi aboli l'ancienne distinction entre les fichiers publics et privés au profit d'une différenciation des régimes sur le fondement de la dangerosité du traitement.

Les flux trans-frontières de données vers un pays tiers à l'Union européenne sont possibles qu'à la condition que le pays de destination garantisse un niveau de protection «adéquat » aux informations reçues.

Les sanctions applicables[9] sont revues à la hausse.

Gérard Gouzes conclue que la « *loi nouvelle sera plus contraignante dans un contexte plus liberticide* » et inscrit cette réflexion dans le cadre des récentes interventions de la Federal Trade Comission (FTC) américaine[10]. Cette loi, pour contraignante qu'elle soit, reste nécessaire au développement de l'Internet. Gérard Gouzes évoque alors les propos de Guy Braibant : Comme le code de la route n'a pas tué l'automobile, la réglementation des traitements de données personnelles ne tuera pas le commerce, avant de rappeler que le projet de loi est encore susceptible d'être modifié lors la procédure parlementaire.

---

[7] Numéro d'identification au sein du répertoire national d'identification des personnes physiques.
[8] Sur les causes de ce retard : voir supra
[9] décret du 23 décembre 1981 et code pénal article 226-16 à 226-22.
[10] Qui a pu faire l'expérience des limites de l'autorégulation.

Auteur : Julien Le Clainche
julien@droit-ntic.com

9h30 – 10h00

LA REFONTE DU REGIME DE DECLARATION A LA CNIL

Par Etienne Drouard, Cabinet Gide Loyrette Nouel

La procédure de déclaration prévue en 1978 reposait sur la distinction entre la nature publique ou privée du traitement des données. Désormais, la distinction se fera au regard de la dangerosité du traitement.

Sous l'empire de la loi de 1978 les traitements de données personnelles de nature privée devaient être déclarés à la CNIL, celle-ci délivrait alors un recipisse attestant que la déclaration avait été effectuée, mais ne garantissait pas la conformité au regard des dispositions impératives de la loi.

Les traitements de nature publique étaient, quant à eux, soumis à une procédure d'autorisation préalable par la CNIL, dont l'avis défavorable ne pouvait être surmonté que par un décret en Conseil d'Etat.

Le projet de transposition de la directive vient complexifier ces situations simples. En effet, s'il peu sembler qu'à la distinction traitement public (soumis à autorisation) / traitement privé (soumis à simple déclaration) succède la distinction « traitement dangereux » / « traitement courant », c'est en réalité sept nouveaux régimes qui sont introduis en droit français.

L'exonération de déclaration par loi et par la CNIL

Seront exonérés de l'obligation de déclaration au terme du projet de loi :

- Les traitements de données relatives aux membres et correspondants d'association et des partis politiques ;
- Les traitements ayant pour objet la tenue d'un registre public destiné à l'information du public. Ex : liste électorale, registre du commerce et des sociétés…

En outre, la CNIL dispose du pouvoir de dispenser de l'obligation de déclaration certaines catégories de traitements.

La déclaration simplifiée

Les dispositions permettant à la CNIL d'adopter des mesures de simplification des formalités de déclaration pour certaines catégories de traitements subsistent, en l'Etat actuel du projet de transposition de la directive 95/46 dans l'ordre juridique français.

L'autorisation par la CNIL

Certaines catégories de traitements appellent une plus grande vigilance et leur création est soumise à une autorisation préalable. Il s'agit :

- Des traitements portant sur des données sensibles telles que définies à l'article 31 de la loi.
- Des traitements portant sur des données génétiques ou biométriques.

Il peut également s'agir :

- Des traitements dits « d'exclusion » : Liste de mauvais payeurs, outils d'analyses du risque financier, traitements comportant des appréciations sur les difficultés sociales des personnes, fichiers privée de lutte contre la fraude…
- Des interconnexions entre des fichiers ayant des finalités différentes.

Etienne Drouard souligne « … *ne relèveront pas de ce régime les traitements mis en œuvre par le secteur public qui comporteraient le numéro de sécurité sociale (le NIR) ou qui porteraient sur la totalité ou la quasi-totalité de la population française, lesquels seront soumis à une autorisation du Conseil d'Etat. A suivre le projet de loi, plus une interconnexion est sensible, plus elle échappe au contrôle de la CNIL.* »

L'autorisation par le Conseil d'Etat

Seront soumis à un régime d'autorisation par décret en Conseil d'Etat, les traitements mis en œuvre par les services de l'Etat :

- Portant sur des données sensibles ;
- Comportant le NIR ;
- Ou qui concernent la totalité ou la quasi-totalité de la population française ainsi que les interconnexions de fichier de cette nature ;

Etienne Drouard note que l'autorisation par la CNIL n'est alors pas nécessaire, celle-ci se bornant à émettre un avis « motivé et publié ». Ainsi, le projet de loi procède à une « *substitution de l'organe décisionnaire* » au profit du Conseil d'Etat et au détriment de la CNIL. En effet, la loi actuelle exige un double avis conforme à la fois du Conseil d'Etat, mais aussi de la CNIL.

L'autorisation par soi-même

Pour étonnante que puisse paraître la formule, c'est ainsi qu'Etienne Drouard décrit la procédure des articles 26.I et 27.II du projet de modification de la loi Informatique et libertés : « *le gouvernement n'a pas craint de prévoir que seraient autorisés par simple arrêté ministériel, c'est à dire par le ministre responsable du fichier en cause,*

- *(i) tous les traitements publics de police et de justice ne comportant pas de données sensibles, ainsi que les traitements qui intéressent la sûreté de l'Etat*
- *(ii) Tous les traitements publics qui nécessitent l'utilisation du numéro de sécurité sociale, ainsi que,*
- *l'ensemble des interconnexions de fichiers publics permettant d'apprécier l'ouverture d'un droit ou l'assiette ou le recouvrement de l'impôt ou l'établissement de statistiques.* »

La CNIL est renvoyée à un rôle consultatif.

La déclaration ordinaire

Ce régime est applicable à tous les traitements de données personnelles ne s'inscrivant pas dans le champ d'applications des régimes précédemment évoqués.

Regrets

Etienne Drouard regrette que la réforme ne soit pas plus simple après une gestation si longue, il évoque notamment les 239 renvois à d'autres dispositions. Il déplore également que les recommandations de Guy

Braibant quant à l'exonération de l'obligation de déclaration pour les traitements les plus courants n'aient pas été suivies.

Etienne Drouard regrette également qu'au terme de l'actuel projet de loi le contrôle des fichiers publics soit relâché et s'interroge sur la compatibilité des ces dispositions avec l'article 8 de la charte des droits fondamentaux de l'Union européenne et l'article 28 de la directive 95/46. Il reste cependant optimiste quant à l'issue du débat parlementaire.

Auteur : Julien Le Clainche
julien@droit-ntic.com

10h00 – 11h00

QUELLES NOUVELLES CONTRAINTES POUR L'ENTREPRISE ?

Modérateur : Christophe Agnus, Transfert

Avec :

- Stéphane Marcovitch, directeur juridique de Wanadoo portails
- Henry de Maublanc, président de l'ASCEL (Association pour le commerce et les services en ligne).
- Dominique Moreno, responsable du département de droit public et économique à la CCIP.

Christophe Agnus :

S'agit-il de nouvelles contraintes ou de la prise en considération soudaine, par les entreprises, de contraintes déjà anciennes ?

Henry de Maublanc, président de l'ASCEL (Association pour le commerce et les services en ligne) :

La loi Informatique et libertés est bien connue tant des professionnels que désormais des consommateurs. Il faut cependant distinguer son appréhension par les groupes de société de sa perception par les petites et moyennes entreprises (PME). Si les grands groupes sont, depuis un certain temps déjà, au fait de la protection des données personnelles, la loi reste encore mal connue par les PME qui la découvre et la pratique seulement depuis quelques années, voir quelques mois. Henry de Maublanc insiste sur l'approche pragmatique des entreprises qui découvrent non pas la loi, mais son application.

Toutefois l'ensemble des entreprises prennent conscience de « l'explosion de la valeur numérique ».

Désormais, c'est le traitement de l'information qui représente la valeur du service.

Henry de Maublanc prend l'exemple de son expérience personnelle : Aquarelle.com est un site sur lequel, le client choisit un bouquet de fleurs afin de le faire livrer à la personne de son choix, accompagné d'un message à caractère personnel. Pour le client, ce qui importe, c'est d'être assuré que sa commande sera livrée dans le délai imparti à la personne désignée, voir, de pouvoir suivre son parcours en temps réel. Les caractéristiques essentielles du service transcendent donc le simple aspect esthétique du bouquet. La vraie valeur du service repose sur le traitement d'informations à caractère personnel. Les consommateurs étant de plus en plus sensibilisés à la protection des informations qui les concernent, l'essor des entreprises dépend du degré de CONFIANCE qui leur est attribué.

La confiance repose :

- Sur une vision éthique des traitements de données ;
- Sur une vision pratique, permettant notamment de garantir la sécurité et la confidentialité des données.

Si la prise en considération de ces deux paramètres ne semble pas poser de difficultés spécifiques aux grands groupes de société, Henry de Maublanc est, en revanche, plus réservé quant à leur appréhension par les PME. En effet, il craint que le manque de sensibilisation soit un obstacle difficile à surmonter.

Auteur : Julien Le Clainche
julien@droit-ntic.com

Henry de Maublanc fait ensuite la constatation que du problème de la sécurité des paiements, encore central il y a quelques mois, les préoccupations des internautes se sont déplacées vers la protection des données personnelles. En effet, la peur du paiement se réduit :
En 1999 25% des internautes avaient effectué un achat en ligne, 15% en 2000[11], pour atteindre 30% en 2001.

Pour finir henry de Maublanc rappelle qu'en matière de protection des données personnelles la sécurité est un enjeu de la confiance.

Dominique Moreno, responsable du département de droit public et économique à la CCIP :

La protection des données personnelles est soumise à une double problématique : Assurer d'une part l'essor du commerce et d'autre part, veiller au respect des droits des personnes. C'est donc dans un souci d'équilibre que la CCIP a donné son avis sur le projet de loi de transposition de la directive 95/46 dans l'ordre juridique français.

Quant au champ d'application du projet, la CCIP a insisté sur :

- La neutralité technologique du projet ;
- L'exclusion des personnes morales de son champ d'application ;
- Une large couverture territoriale : le simple recours à des moyens en France devant suffire à justifier l'application de la loi française.

La CCIP a œuvré en faveur de la consécration textuelle des principes :

- De licéïté ;
- De finalité ;
- De légitimité.

La CCIP a, par ailleurs, plaidé pour une autorégulation coordonnée par la CNIL parallèlement aux évolutions législatives. Dominique Moreno cite alors le contrat type de commerce électronique rédigé par la CCIP en exemple.

Quant aux nouvelles formalités préalables, la CCIP salue la distinction nouvelle au regard de la dangerosité potentielle du traitement et milite pour une exonération pour certaines catégories de traitements « professionnels » : seuls les fichiers clients devraient être protégés strictement.

Sur les modalités d'exercice des droits à l'information, d'accès et de rectification, la CCIP rejoint la position de la CNIL :

- Case à cocher,
- Information claire sur les techniques de correction,
- Information claire sur les protections juridiques et techniques des données,
- Accès facile aux zones d'exercice des droits d'accès, d'opposition
- Facilité d'accès à l'information relative au traitement.
- Possibilité de filtrage des recours manifestement abusifs.

[11] Il faut noter que le nombre des internautes avait considérablement augmenté.

En revanche, la CCIP CONTESTE le pouvoir de sanctions pécuniaires attribué à la CNIL au terme du projet de loi. Elle prend position contre une extension du pouvoir répressif : Il existe déjà un arsenal pénal sévère en matière de protection des données.
Cette position a été le point de départ d'un débat avec l'auditoire, les uns arguant de la non-application des dispositions pénales existantes, raisonnant par comparaison avec d'autres autorités administratives indépendantes (Commission des opérations de bourses, le Conseil de la concurrence…), analysant la situation dans d'autres ordres juridiques, notamment aux Etats-Unis. Les autres s'inquiétant de la tendance à dépouiller les juridictions de leurs prérogatives.

Sur le thème des flux trans-frontières de données, la CCIP s'inquiète de l'évolution pratique de l'accord « Safe harbor » conclu entre l'Europe et les Etats-Unis, pourtant entré en vigueur depuis le 9 novembre 2000. Elle se réjouit néanmoins de la reconnaissance textuelle de la « protection adéquate » et demande la négociation d'un accord international dans le cadre de l'ONU ou de l'OCDE, pour parvenir à un « *tronc commun* » pour la protection des données personnelles.

Stéphane Marcovitch, directeur juridique de Wanadoo portails :

Quelles sont les nouvelles contraintes pour l'entreprise ? Pour Stéphane Marcovich, il en est essentiellement trois :

1. Les contraintes de marché :
Il s'agit de gagner la CONFIANCE des clients de manière à mieux les satisfaire en procédant à des traitements de données personnelles nécessaires au développement des services fournis par l'entreprise.

2. Les contraintes issues des formalités de déclaration :
Dans l'esprit du rapport « Braibant » et de la majorité des intervenants de cette journée, Stéphane Marcovich a souligné les contraintes que représentaient aujourd'hui, les formalités nécessaires hier et a regretté l'absence de simplification dans le projet de loi.

3. L'information :
Stéphane Marcovich insiste sur la difficulté pour les entreprises, surtout les PME, de respecter les dispositions relatives à l'information des personnes. En effet, l'information pour être satisfaisante doit être adaptée à la personne. Or, la clarté est un objectif qui n'est pas toujours atteint par les entrepreneurs individuels.

Henry de Maublanc

Pour conclure cette intervention Henry de Maublanc a rappelé que l'aléa dans la visibilité sur le Net d'une entreprise rendait, plus que jamais, la confiance dans la marque nécessaire, avant de poursuivre que la « traque » n'est guère positive pour le commerce.

Auteur : Julien Le Clainche
julien@droit-ntic.com

11h30 – 12h15

QUEL CONTROLE DE L'ETAT ?

Modérateur : Bertrand Nouel, Cabinet Gide Loyrette Nouel

Avec :

- Sébastien Canevet, Maître de conférences en droit privé.
- Maurice Ronais, rapporteur du livre blanc « Administration électronique et protection des données personnelles ».

Bertrand Nouel :

« Sommes-nous 'stiqué' ? », Autrement dit, figurons-nous dans le Système de Traitement des Infractions Constatées (STIC) ? Ce fichier, crée en 1993, Répertorie les auteurs d'infractions de cinquième classe. Pourtant, pas moins de six millions de personnes y sont inscrites, soit environ un français sur dix. Il est souvent apparenté à une sorte de second casier judiciaire.

La CNIL a mené une action importante, notamment quant à l'accès aux informations et leur durée de conservation, pour protéger les personnes de la menace que STIC pouvait représenter pour leur vie privée. Avant les interventions de la CNIL, les témoins figuraient également dans ce fichier, ce qui le rendait plus complet que le casier judiciaire. La CNIL semble payer aujourd'hui son combat d'hier pour la mise en conformité de STIC. En effet, au terme du projet de loi, la CNIL voit ses pouvoirs sur l'Etat se réduire : Un service de l'Etat pourra s'affranchir de l'autorisation de la CNIL par celle du ministre compétent pour la création ou l'interconnexion de fichiers. Ce qui revient à une procédure « d'auto-autorisation » susceptible d'être incompatible avec l'article 8 de la charte des droits fondamentaux de l'Union européenne.

Maurice Ronais, rapporteur du livre blanc «administration électronique et données personnelles » :

Administration électronique : Quel identifiant choisir ?

L'objectif de l'administration électronique (ou e-administration) est de permettre une entrée personnalisée, un guichet unique, pour l'ensemble des démarches administratives[12]. Il s'agit d'une réforme profonde et ambitieuse de l'administration française qui se construit « *autour du citoyen et non pour le citoyen* ». Cette réforme implique des efforts tant techniques que budgétaires : « *d'une administration en silo, nous passons à une administration en réseau.* »

La circulation des données :
Les différents services de l'administration nous envoient régulièrement quérir, auprès d'un de leurs homologues, une pièce qu'ils ne peuvent se procurer eux-même. Si les services pouvaient faire circuler l'information tout en garantissant sa confidentialité et son intégrité le gain de temps serait appréciable, tant pour l'usager que pour l'administration.

La menace de l'Etat à l'origine des législations sur les données personnelles n'est plus d'une actualité aussi aiguë que dans les années soixante-dix : « *Les risques et les inquiétudes en matière de vie privée se sont*

[12] Voir : http://www.monservicepublic.fr

déplacés des 'grands fichiers' vers les 'traces', des administrations, vers les opérateurs privés.» De nouvelles formes de collectes se sont développées notamment sur les réseaux, la puissance des moteurs de recherche permet d'opérer des croisements d'informations, les flux de données augmentent considérablement sous l'influence du marché que représente leur commerce. Maurice Ronais a ensuite mis en exergue la « *complémentarité de la loi et de la technologie dans la protection de la vie privée*» en illustrant son propos par l'exemple américain caractérisé par la foi en la technologie et dans la responsabilisation des individus.

Désormais, la sauvegarde de la vie privée se fait par une double approche de la protection des données :

- Une protection « par le haut » : loi, autorité administrative indépendante…
- Une protection « par le bas » : C'est une protection exercée par les personnes elles-mêmes : droit à l'information, droit d'accès et de rectification…

L'administration électronique nécessite le recours à des identifiants. Ceux-ci doivent répondre à des impératifs de :

- Transmission ;
- De reconnaissance ;
- De suivi.

Le progrès technologique amène à une multiplication des identifiants (signature électronique, adresse IP, pseudonymes…) qui n'est pas sans conséquences :

- Comment mémoriser cette multitude d'identifiants ?
- Comment les rendre inter-opérables entre eux ?
- Comment maîtriser la circulation des données personnelles associées ?

Ces besoins se traduisent par l'émergence de nouvelles prestation de service sur la « marché de la confiance ». La délivrance et le contrôle d'identité étant des prérogatives régaliennes, le rôle de l'Etat et de nouvelles procédures sont à redéfinir.

L'identité publique est « *un processus qui relie des registres (l'état civil), une combinaison d'information (reliées au patronyme), des éléments matériels détenus par les administrations (photographie numérisée, empreinte digitale…) et des titres d'identité.* » Le lien peut varier selon les ordres juridiques considérés, ainsi, aux Etats-Unis il n'existe pas de carte d'identité.

La refonte de la procédure d'attribution de l'identité publique doit être orientée vers une sécurité accrue (procédure du titre fondateur) et vers le développement d'une « gamme » de carte d'identité :

- Carte d'identité nationale simple,
- La carte nationale d'identité électronique,
- La carte du citoyen (CNIE + carte d'électeur),
- La carte du conducteur (CNIE + droit de conduire),
- Le passeport simple,
- Le passeport électronique.

Des expériences dont le fonctionnement repose sur des cartes « électroniques », notamment cartes à puce ont été mené en Finlande, en Suède et en Italie et sont en projet en Belgique ainsi qu'en Allemagne.

L'administration électronique proposera aux usagers d'accéder à des « téléservices intelligents.» :

- Le formulaire permettra le contrôle des champs,

- Permettra l'échange d'information entre les administrations, afin de ne pas demander des pièces déjà détenues par un autre service.
- Permettra à l'usager d'accéder à un « compte administratif personnalisé » servant notamment, à l'exercice du droit d'accès.
- Le dossier permettra de conserver des traces des échanges intervenus entre l'usager et l'administration.
- Des services transversaux aux différentes administrations seront développés, par exemple, la déclaration en ligne du changement d'adresse. Ce service ayant été expérimenté au Canada et dans la province de Québec.
- Ces « télé-services intelligents » seront inter-opérables avec des télé-services privés. Toutefois une attention particulière devra alors être portée à l'authentification et la gestion des identités numériques.

Sébastien Canevet : maître de conférence en droit privé

Après avoir exposé les modifications apportées par le projet de loi aux formalités préalables à la constitution de fichiers publics, particulièrement les fichiers touchant à la sécurité de l'Etat, Sébastien Canevet a expliqué la logique générale du projet de loi :
Il a regretté l'excessive modération de la CNIL quant à la création de fichiers de publics. Il a cependant souligné que l'audace de la commission lui valait une restriction de son pouvoir de contrôle sur l'Etat, s'insurgeant contre le régime « d'auto autorisation » ministérielle. Cette perte de pouvoir est loin d'être compensée par la maigre avancée, en matière de droit d'accès aux fichiers de police, réalisée par l'article 41 du projet de loi.

La loi sur la sécurité quotidienne (LSQ) est intervenue pour lutter contre le sentiment d'insécurité. L'arsenal pénal sert à lutter contre les infractions, mais est-il réellement adapté à la lutte contre un sentiment ? c'est dans ce contexte que dix nouvelles mesures répressives « justifiées » par les attentats du 11 septembre 2001 ont été introduites. Après avoir déploré le manque de contrôle démocratique de la procédure parlementaire en général[13], Sébastien Canevet s'est indigné de l'inconstitutionnalité particulière de la loi sur la sécurité quotidienne, les députés ayant été privé d'une première navette parlementaire.

Les dispositions introduites, en cours de discussion, à la LSQ portaient notamment sur la conservation des « fichiers log. » D'une part, la loi ne définit pas ce qu'est précisément un « fichier log », d'autre part, pour Sébastien Canevet, leur conservation excessive dans le temps a pour conséquence la fin de l'anonymat sur les réseaux. Cette disposition de la LSQ semble donc être en contradiction avec l'article 6-1 de la directive 97/66[14] qui impose l'effacement des traces à la fin de la connexion.

Le débat avec l'auditoire a porté sur les modalités techniques du traitement de « données de surf », travail titanesque et coûteux.

Nous changeons de modèle politique. D'une logique démocratique (procès…) nous passons avec l'enregistrement systématique à une logique policière et non-démocratique.

[13] 95% des lois votées sont issues de projets de loi émis par le gouvernement.
[14] Directive 97/66 CE du Parlement européen et du Conseil du 15 décembre 1997 portant sur la protection des données à caractère personnel et la vie privée dans le secteur des télécommunications.

La problématique répressive est bloquée entre des juridictions judiciaires qui sanctionnent faiblement les atteintes à la protection des données personnelles et la logique des autorités administratives indépendantes qui est de punir sans juger.

Louise Cadoux est alors intervenue pour souligner qu'elle n'accordait pas sa confiance à l'administration électronique et qu'en conséquence elle ne ferait pas sa déclaration d'impôts en ligne : « *L'administration des impôts est dispensée de la communication des informations.* » Elle s'est élevée contre les artifices du ministère des finances : « *Bercy ment ! l'OCDE n'exige pas la création d'un numéro commun…* ».

Auteur : Julien Le Clainche
julien@droit-ntic.com

12h15 – 12h35

SERVICES ELECTRONIQUES DE LA VILLE ET PROTECTION DU CYBER-CITOYEN

Présentation par Pascal Cazabat, directeur technique de T.R.I.S, Groupe Adesium

Exemple d'un télé-service

Le principe selon lequel la sécurité des citoyens ne peut se faire qu'avec le recours à une carte à puce ne correspond pas à une réalité du marché. Il faut hiérarchiser les besoins de sécurité.

L'exemple du permis de construire : Il y a deux hypothèse, soit l'autorisation est données par le maire, soit par la direction départementale de l'équipement (DDE). La procédure d'attribution des permis de construire donne lieu à de nombreux échanges entre le demandeur et le service compétent qui peut solliciter un complément d'information sur le projet.

Objectifs

- Démontrer l'utilité d'un télé-service,
- Garantir un niveau de sécurité adapté ;
- Responsabiliser les usagers.

Le dépôt

1. Identification de la personne physique à la mairie ;
2. Support : carte à puce (50 à 100 €) pour garantir la confidentialité des informations et empêcher leur recoupement.

Enregistrement de l'utilisateur

L'information la plus importante est l'adresse électronique de l'usager. Ainsi, La Poste avait-elle prévu de proposer une adresse électronique à chaque français.

Il existe deux types de besoins :

1. Besoin d'identification,
2. Un besoin de signature : problématique du consentement.

Deux niveaux de sécurité ont été développés :

1. Une sécurisation par recours à la carte à puce ;
2. Une sécurisation alternative par disquette physique et reproductible.

Création du dossier

- Création d'un compte personnalisé ;
- Création d'un dossier répertoriant les échanges effectués.

Les échanges sont validés par signature des pièces associée à un processus d'authentification (signature électronique, certification…)

14h15 – 15h15

LA CYBERSURVEILLANCE DES SALARIES

Modérateur : Joël Grangé, Cabinet Gide Loyrette Nouel

- Hubert Bouchet, vice-président de la CNIL
- Nathalie Moreau, directrice juridique de l'institut européen de sécurité des systèmes d'information
- Guy Lapassat, animateur du club « Nouvelles technologies » du Giref (Club informatique des grandes entreprises françaises)

Hubert Bouchet, vice-président de la CNIL

La CNIL a rendu public deux rapports successifs sur le thème de la cybersurveillance du salarié[15]. Ces deux études ont été rendues nécessaire par l'évolution rapide des pratiques et de la jurisprudence. Le premier rapport comprenait dix sept contributions formelles et avait pris en compte vingt cinq mille participations publiques enregistrées sur le site de la CNIL.

Si le principe veut que le salarié ne s'adonne qu'à son activité professionnelle sur son lieu de travail. A cet Homme sont reconnues des droits et des libertés, même sur le lieu de son activité professionnelle. C'est déjà ce qu'affirmait la « loi Auroux » de 1982 en reconnaissant que le règlement intérieur pouvait connaître des limitations.

Cette prise en compte des droits des salariés sur leur lieu de travail aboutit à :
- Une rationalisation des procédures de recrutement ;
- L'application du principe de proportionnalité ;
- Le respect du principe de loyauté.

Le développement social engendre une métamorphose du travail qui devient plus intellectuel et moins physique. La surveillance du salarié a donc, elle aussi évoluée : ordinateurs, badges et vidéo surveillance laissent désormais la place aux architectures en réseaux permettant la traçabilité. Une réflexion sur les conditions d'efficacité du travail intellectuel doit donc être menée.

L'employeur est dans une logique de surveillance et le salarié dans une logique de protection de la vie privée. Si le salarié voit ses droits s'étendre, il faut rechercher un nouvel équilibre entre la liberté et le devoir.

Il existe une corrélation entre la productivité et le respect de la vie privée du salarié. Ainsi, la CNIL prend position pour un contrôle non du contenu des échanges, mais de leur volume. En effet, un comportement abusif se traduit souvent par des flux anormaux. L'administrateur réseau a alors un rôle de « chef de gare », il ne contrôle pas tous les usagers mais le fonctionnement normal des « trains ».

Le rôle de l'administrateur réseaux est central mais, force est de constater qu'il est encore mal protégé contre les pressions éventuelles qu'il pourrait subir en vue d'une communication d'informations protégées.

[15] Rapport du 28 mars 2001 et rapport du 18 février 2002.

Même si l'usage personnel de l'ordinateur professionnel est sujet à moins de litiges, la CNIL veut que dans chaque société de taille respectable il y ait un « référent données personnelles », c'est à dire une personne spécialement affectée à la gestion des traitements de données personnelles. La surveillance peut être stratégique, notamment lors des négociations sociales.

Hubert Bouchet conclue que du « connais-toi, toi-même » de Socrate nous sommes passés à une logique de « Connaissez les vous-même »…

Modérateur : Joël Grangé, Cabinet Gide Loyrette Nouel

La surveillance doit exister, mais à bon escient. L'arrêt « NIKKON »[16] est symptomatique. Un salarié avait envoyé des documents professionnels sous couvert d'expédier un « courrier personnel ». L'employeur ayant ouvert le courrier a pu constater le comportement abusif mais n'a pu le faire valoir. En effet, l'ouverture d'un courrier personnel est prohibée par l'article 8 de la Convention 108 du Conseil de l'Europe[17] et par l'article 9 du code civil. Cette jurisprudence crée un risque, mais la règle n'est pas immuable et appelle discussion, voir une intervention législative.

Guy Lapassat, animateur du club « Nouvelles technologies » du Giref (Club informatique des grandes entreprises françaises)

Il y a trois niveaux :
- La société ;
- L'entreprise;
- Les techniciens.

L'établissement d'un « référent CNIL » ne pose pas de problèmes particuliers dans les grandes sociétés.

Le recours au cryptage, aux firewall et aux anti-virus ne suffit pas toujours à résister au piratage. En outre, l'administrateur réseau peut tricher sans le PDG alors que l'inverse est moins courant. Il existe des méthodes douces, notamment le dialogue et la négociation, qui permettent d'éliminer un grand nombre de comportements abusifs. Resteront alors, les comportements réellement dangereux, dont l'espionnage industriel souvent mené par un technicien interne à la société. C'est contre ceux là qu'il est le plus difficile de lutter.

Modérateur : Joël Grangé, Cabinet Gide Loyrette Nouel

N'existe-t-il pas une contradiction entre la demande de transparence sans cesse plus importante et des règles juridiques encore floues ? Comment concrétiser les principes développés par le rapport de CNIL rendu public en février 2002 ?

1. Principe d'information préalable.
2. Discussion collective préalable.

[16] Cass.Soc, 2 octobre 2001 : arrêt "NIKON" , les conclusions de M.KEHRING.
[17] Convention 108 du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard des traitements automatisés de données à caractère personnel.

3. Principe de proportionnalité.

Le principe de proportionnalité est le plus difficile à mettre en œuvre tant il relève d'une appréciation subjective. Des « pistes » ont été dégagées par la CNIL :

- Pas de contrôle individuel mais surveillance du volume des échanges ;
- Les fichiers de journalisation ne doivent pas être conservés plus de six mois ;
- Le rôle des administrateurs réseau : indépendance et contrôle sont indispensables, mais difficiles en pratique ;
- Accords collectifs sur les techniques de surveillance ;
- Référent CNIL ;
- Bilan annuel informatique et libertés;

Hubert Bouchet, vice-président de la CNIL

En l'absence de réglementation claire, il doit exister des pratiques vertueuses, l'indépendance de l'administrateur réseau doit être garantie, le bilan annuel permet de suivre l'évolution sur une année… Il doit exister une information sur l'exploitation des biens immatériels des personnes. Les syndicats auront un rôle à jouer dans les évolutions à venir.

Guy Lapassat, animateur du club « Nouvelles technologies » du Giref (Club informatique des grandes entreprises françaises)

La vision classique est manichéenne, l'entreprise est forte, le salarié est faible. Pourtant, il peut arriver (un cas sur cent) que le faible abuse de sa position de manière dangereuse pour l'entreprise, il faut donc un système de surveillance et de contrôle souple et adaptable.

Le contrôle du volume des échanges et de l'accès aux zones privatives sont essentiels. Toutefois, monsieur Lapassat regrette que la conservation des informations ne puissent excéder six mois.

15h15- 16h30

MARKETING, BASES DONNEES ET VIE PRIVEE

Modérateur : Christophe Agnus, Transfert

Avec :

- Laurent Alexandre, fondateur de Medcost ;
- Georges Fisher, directeur de la direction des TIC et du commerce électronique à la CCIP ;
- Serge Gauthronet, sociologue, directeur de l'agence ARETE
- David Nataf, président de l'Institut européen de sécurité des systèmes d'information ;
- Alain Reminiac, directeur général d'Adesium.

Serge Gauthronet, sociologue, directeur de l'agence ARETE :

Le développement des collectes de données à caractère personnel à des fins commerciales, notamment la création des « Data warehouse » est préjudiciable au consommateur. L'efficacité des techniques marketing utilisant les bases de données n'est pas démontré. En effet, seulement 0,5% des internautes cliquent sur les bannières de la célèbre société de profilage et de vente d'espace publicitaire Doubleclick. Le retour sur investissement est donc très aléatoire alors que les compétences requises sont coûteuses et techniquement complexes. Ces méthodes peuvent, également, être préjudiciables à la société en terme d'image.

En outre, nombre de traitements ont été réalisés à une époque à laquelle la vente des fichiers était rarement envisagée. L'exemple de Toysmart est illustratif : La société de jouets américaine après être tombée en faillite souhaitait vendre son fichier « client » fort de 250.000 entrées. Les personnes concernées n'ayant pas été informées, de l'éventuelle cession au moment de la collecte, la vente n'a pu être réalisée et le fichier a du être détruit.

La loyauté de la collecte est prépondérante :

- Consentement des personnes ;
- Information des personnes ;
- Respect de la finalité et du contexte…

La protection des données à caractère personnel est donc nécessaire au développement du marketing. Un marché publicitaire confus est inefficace : Une personne exposée à un nombre excessif de messages à caractère publicitaire leur devient imperméable. Il faut développer le « marketing de consensus ».

Alain Reminiac, directeur général d'Adesium

Après avoir abondé dans le sens de Serge Gauthronet, Alain Reminiac a distingué les mesures destinées à protéger le salarié de celles relevant de la prospection des citoyens. Le fichier client d'une société n'est pas cessible, mais constitue cependant un élément d'actif.

Auteur : Julien Le Clainche
julien@droit-ntic.com

Georges Fisher, directeur de la direction des TIC et du commerce électronique à la CCIP ;

Pour Georges Fisher, il importe de distinguer la réalité de la perception. Par exemple, si la vente d'un fichier est assortie d'une clause garantissant moins de 3% de retour motivé par le changement d'adresse, celle-ci rassure et dans l'hypothèse d'un dépassement, sera pourtant rarement invoquée.

Il importe également de distinguer les relations des entreprises entre-elles (B to B), de leur relations avec leurs clients (B to C). Dans une relation B to B, l'objectif poursuivi est de créer des contacts entre les entreprises alors que dans le cadre d'une relation avec le client, l'objectif est la vente. Des labels spécifiques aux relations B to C sont entrain de se développer.

Un label doit garantir :

- Une certaine utilisation des données personnelles,
- Le respect des normes en vigueur,
- Le respect des dispositions contractuelles (délai de livraison, prix…)

Pourtant, force est de constater que les labels sont encore peu développés en pratique, le spam et le paiement occultant souvent les problèmes liés aux traitements de données personnelles.

En outre, se pose un problème de faisabilité réelle. Parmi les nouveaux outils,(One to tribe, one to one…), peu ont démontré leur efficacité.

Les relations que doivent entretenir le marketing et la vie privée doivent être équilibrées. D'une part, ces techniques peuvent représenter un profit pour le consommateur, mais peuvent d'autre part, se traduire par une menace planant sur la vie privée. L'arbitrage devra se faire à la lumière :

- Du principe de finalité,
- Du droit à l'information.

David Nataf, président de l'Institut européen de sécurité des systèmes d'information

David Nataf à ouvert son allocution en regrettant le manque d'intérêt suscité par les questions relatives à la vie privée. La loi de 1978 et les dispositions pénales participent d'un arsenal législatif complexe mais garantissant une protection efficace. La sécurité des informations bancaires est également un sujet de préoccupation alarmant, la carte de bleu étant qualifiée de « *éminemment pas fiable* ».

Il est étonnant que le système Echelon n'ait pas créé une mobilisation de masse pour la protection des données personnelles en Europe. Si les moyens législatifs et techniques ne manquent pas, « *c'est la volonté qui n'est pas au rendez-vous.* »

Serge Gauthronet, sociologue, directeur de l'agence ARETE :

Serge Gauthronet a conclu par une référence à François Rigaud, rappelant la liberté de maîtriser « *l'image de soi* ».

Auteur : Julien Le Clainche
julien@droit-ntic.com

16h15 – 16h45

GROUPES DE SOCIETE ET FLUX TRANSFRONTIERES DE DONNEES

La gestion mondiale des données personnelles : Quels contrôles pour quels profils ?
Par Etienne Drouard, Cabinet Gide Loyrette Nouel.

Les différents ordres juridiques (Europe, Etats-Unis, japon…) réagissent aux problèmes liés aux traitements de données à caractère personnel. A cet égard, la réaction américaine est symptomatique. Après avoir réglementé très tôt (Privacy Act de 1974) face à la menace des administrations, les Etats-Unis semblent lancés dans un mouvement législatif de grande ampleur, pour régir les difficultés dues à une exploitation commerciale des informations nominatives. En effet, non seulement trois projets de loi fédéraux sont à l'étude mais encore, le nombre des lois étatiques relatives au spam est passé de 28 en 1999 à 40 en 2002. Ainsi, le spam est-il considéré Outre-Atlantique comme une utilisation frauduleuse de l'identité de la personne passible d'une amende de 1000 $ par infraction constatée.

Deux solutions doivent être distinguées dans le cadre d'un flux transfrontières de données vers un pays n'appartenant pas à l'Union européenne :

- Le flux se fait vers un pays destinataire offrant une protection « adéquate » aux informations.
- Le flux est régit par un contrat de transfert de données personnelles.

Le projet de loi devant modifier la loi informatique et libertés transpose les articles 25 et 26 de la directive 95/46. Du critère de la protection équivalente, nous passons à la nécessité d'une protection adéquate des données par l'ordre juridique destinataire.

Un niveau de protection adéquat s'entend d'un ordre juridique compatible avec les exigences européennes.

Les Etats-Unis n'ayant pas été considérés comme offrant un niveau de protection adéquat, un large débat s'est ouvert. En effet, cette décision est susceptible de créer des difficultés au sein des groupes de société internationaux ayant des intérêts en Europe.

Une solution à donc été négocié par la Feraral Trade Comission (FTC) et la Commission européenne. Il s'agit de l'accord « Safe harbor » entré en vigueur depuis le 9 novembre 2000. Au terme de cet accord, les sociétés américaines ont la possibilité d'adhérer à un socle de principes et sont alors considérées comme offrant un niveau de protection adéquat.

L'évolution de cet accord est incertaine. En effet, la FTC et l'administration du président Bush exercent des pressions sur la Commission européenne pour obtenir plus de souplesse. En outre, seules 154 entreprises ont adhérées à cet accord. Ainsi, certains s'interrogent sur l'avenir de la « sphère de sécurité ».

Une solution alternative se présente sous la forme du contrat de transfert de données à caractère personnel.

- Il se traduit par une contractualisation de la loi,
- Il doit être approuvé par une autorité indépendante,
- Il doit garantir le respect de la finalité du traitement.

La directive et le projet de loi prévoient que le transfert vers un pays n'offrant pas un niveau de protection adéquat peut être valider par le consentement de la personne.

Auteur : Julien Le Clainche
julien@droit-ntic.com

D'autres dérogations sont possibles, lorsque le transfert est nécessaire à l'exécution d'un contrat entre la personne concernée et le responsable du traitement ou à l'exécution d'un contrat ou de mesures pré-contractuelles, dans l'intérêt de la personne, entre le « maître du fichier » et un tiers.

Les groupes de société sont soumis à des problématiques spécifiques. Le croisement des données entre entreprises appartenant à un même groupe est assimilé à un transfert à un tiers. Peu importe la détention du capital. Cette assimilation est fondée par :

- Le droit à l'information ;
- Le respect du principe de finalité.

Ainsi, la fusion des sociétés Doubleclick et Abascus a pu être interdite aux Etats-Unis, aurait-elle pu être autorisée en France ?

16h45 – 17h15

SYNTHESE ET CONSLUSION

- Patrice Bloche, délégué national du Parti Socialiste PS aux nouvelles technologies de l'information et aux multimédias
- Patrice Martin-Lalande, député du loir et cher, co-président du groupe d'étude sur les NTIC.

Patrice Bloche, délégué national du Parti Socialiste PS aux nouvelles technologies de l'information et aux multimédias

Patrice Bloche a rappelé les évolutions dégagées, notamment par le livre blanc sur « *l 'administration électronique et les données personnelles* » :

- « *Les risques et les inquiétudes en matière de vie privée se sont déplacés des 'grands fichiers' vers les 'traces', des administrations, vers les opérateurs privés.*»
- La « *complémentarité de la loi et de la technologie dans la protection de la vie privée*»,
- La protection « par le haut » : loi, autorité administrative indépendante…
- La protection « par le bas », c'est une protection exercée par les personnes elles-mêmes : droit à l'information, droit d'accès et de rectification…

Patrice Bloche a noté :

- Il s'agit d'une adaptation de la loi et non d'une refonte.
- Il existe une place pour l'autorégulation dans le cadre de la loi.
- Il y a eut une adaptation des moyens de la CNIL, mais aussi des possibilités offertes aux citoyens.
- Une modification du droit de travail est en cours.
- Il s'agit d'un débat politique au sens fort pour une société juste, sûre et moderne qui doit tendre vers l'équilibre et surtout ne pas créer une fracture numérique.

Patrice Martin-Lalande, député du loir et cher, co-président du groupe d'étude sur les NTIC.

Après avoir abondé dans le sens de son collègue à la co-présidence du groupe d'étude sur les NTIC, Patrice Martin-Lalande a souhaité se désolidariser sur quelques points :

- La réduction du contrôle de la CNIL sur les fichiers publics.
- La réduction des informations offertes quant à la finalité du traitement.
- La complexité du projet de loi, qui comporte notamment 239 renvois et créé sept régimes différents de formalité préalable à la mise en œuvre d'un traitement de données à caractère personnel.

Il a ensuite milité pour :

- La reconnaissance textuelle du « principe de pertinence ».
- Le renforcement de l'information des personnes.
- La promotion de l'anonymisation.

Auteur : Julien Le Clainche
julien@droit-ntic.com