L'informatique et les technologies de communication constituent un des moteurs de l'économie et des relations sociales. Elles sont également perçues comme des outils de sécurité publique. Elles constituent, enfin, le ressort d'instruments de confort et de puissance intégrés à la vie quotidienne de chacun de nous.

Ces évolutions rapides, auxquelles nous participons, consciemment ou non, comportent déjà toutes les possibilités de l'identification infaillible de l'homme et du suivi de ses activités individuelles ou collectives réalisées par l'intermédiaire de supports électroniques. Elles défient la loi de 1978 modifiée en 2004 destinée à assurer la protection des libertés et des droits fondamentaux face à l'informatique. Elles interrogent les valeurs attachées à la démocratie dans un monde ouvert tout autant que notre conception de l'homme et de la société.

A l'heure où se cumulent les vagues technologiques dans un contexte de recherche de sécurité collective, ce colloque de réflexion, organisé conjointement par la Commission Nationale de l'Informatique et des Libertés et l'Université Paris II, sous l'égide et avec l'appui du Sénat, a bénéficié des regards croisés et exigeants de représentants de tous les acteurs concernés, français et étrangers : industrie, services, administrations, associations, politiques, commissaires chargés de la protection des données personnelles, universitaires et chercheurs.

Ce volume s'inscrit dans la série de publications destinées à rendre compte des manifestations et colloques institutionnels organisés par le Sénat ainsi que, le cas échéant, par ses commissions ou délégations.
Cette collection est l'expression de la volonté d'ouverture du Sénat. Elle a pour vocation de mieux faire connaître son activité de réflexion et sa force de proposition.

Retrouvez le Sénat sur internet : http://www.senat.fr

ISBN 978-2-11-114149-0

ISSN 1249-4356
Prix de vente au public : 5,00 €

CNIL. Commission Nationale de l'Informatique et des Libertés

SÉNAT

UNIVERSITÉ PANTHÉON-ASSAS PARIS II
DROIT - ÉCONOMIE - SCIENCES SOCIALES

Informatique : servitude ou libertés ?

LES COLLOQUES DU SÉNAT

les actes

7 et 8 novembre 2005

Informatique : servitude ou libertés ?

Colloque organisé au Sénat
sous le haut patronage de M. Christian Poncelet, Président du Sénat,
les 7 et 8 novembre 2005
par la Commission Nationale de l'Informatique et des Libertés (CNIL)
et l'université Panthéon – Assas – Paris II

CNIL. Commission Nationale de l'Informatique et des Libertés

SÉNAT

UNIVERSITÉ PANTHÉON-ASSAS PARIS II
DROIT - ÉCONOMIE - SCIENCES SOCIALES

INFORMATIQUE : SERVITUDE OU LIBERTÉS ?

Colloque organisé au Sénat,
sous le haut patronage de M. Christian Poncelet, Président du Sénat, les 7 et 8 novembre 2005
par la Commission Nationale de l'Informatique et des Libertés (CNIL) et l'université Panthéon – Assas – Paris II

INTRODUCTION DE M. CHRISTIAN PONCELET

Le Sénat a été heureux d'accueillir dans ses murs ce colloque et de s'associer à des travaux qui, à l'image de la qualité et de la diversité des intervenants, ont été d'une grande richesse.

Je saisis cette occasion pour rappeler ici l'importance qu'ont toujours constitués, aux yeux du Sénat, les sujets traités au cours de ces deux jours, et évoquer les liens historiques et personnels qui, depuis sa création, existent entre la CNIL et le Sénat. Peu après sa création c'est d'ailleurs le sénateur Jacques THYRAUD, rapporteur au Sénat de la loi du 6 janvier 1978 et inventeur, à ce titre, de l'expression d' « autorité administrative indépendante », récemment décédé, qui en avait pris la présidence marquant de son empreinte cette institution naissante. Á l'aube d'une profonde réforme de la CNIL, celle de 2004, et alors que son décret d'application vient de paraître, je suis heureux de voir que le Sénat est au rendez-vous en la personne d'un autre président sénateur, Alex TÜRK.

« Informatique : servitude ou libertés ? » cette interrogation ne fait-elle pas écho au titre même de notre loi fondatrice en la matière qu'est la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ? Au cours des trente dernières années, le développement de l'Internet, et plus généralement de l'informatique, a constitué une véritable révolution : la naissance d'une nouvelle ère : celle de *l'Homo Informaticus*.

Ces progrès scientifiques et techniques nous ont permis de nous affranchir de nombreuses contraintes matérielles, notamment en facilitant l'accès à l'information

et son traitement. Ils peuvent aussi constituer des contraintes voire des menaces pour les libertés si des règles ne viennent pas les contenir.

C'est bien à ce carrefour que vous avez choisi de placer votre réflexion, analysant tour à tour ces avancées majeures que constituent l'identification biométrique, la personnalisation des relations commerciales, puis la loi de 1978 profondément rénovée en 2004. Bien entendu, et même si la France peut s'enorgueillir d'avoir été parmi les premières à s'interroger sur ces problématiques et à légiférer en la matière, inspirant ainsi le droit communautaire, la réflexion a su sortir du cadre hexagonal et s'enrichir des autres expériences, qu'elles nous soient proches comme celle de l'Union, ou plus éloignées comme celles des États-Unis d'Amérique, de Russie ou de Chine.

À un moment où nos sociétés ont à faire face au terrorisme, le Parlement examinera d'ici à la fin de l'année le projet de loi qui lui est consacré où l'informatique prend une part de plus en plus grande dans la vie de nos contemporains, qu'ils soient consommateurs, citoyens, administrés, salariés, entrepreneurs, de telles réflexions sont bien sûr utiles mais surtout nécessaires sur les chemins de notre liberté.

LUNDI 7 NOVEMBRE 2005

I. 14H00-14H30

A. ALLOCUTION D'OUVERTURE

1. Allocution de M. Alex TÜRK, Président de la Commission Nationale de l'Informatique et des Libertés

Mesdames, Messieurs, permettez-moi de remercier le Sénat et son Secrétaire général Alain DELCAMP, le Professeur CHAGNOLLAUD ainsi que Dominique WOLTON qui sera présent demain. C'est à partir de rencontres informelles que progressivement s'est développée cette idée de mettre en place un colloque qui nous permette d'approfondir un certain nombre de questions.

Je voudrais maintenant m'exprimer sur le thème « informatique : servitude ou libertés ». Pour vous dire la vérité, j'aurais préféré l'expression « Servitude et libertés ». Peut-être suis-je plus pessimiste que les autres membres de notre petit groupe de réflexion. Il se trouve que j'ai le sentiment que nous vivons aujourd'hui dans une société où la servitude et la liberté se partagent autour de la problématique de l'informatique. C'est déjà pour moi une façon de prendre position dans le débat. Quoiqu'il en soit, cela signifie, à mes yeux, qu'il y a au moins une question sur laquelle il s'agirait d'avancer. Comment en finir avec le mythe du *Big brother* ? Il y a deux façon d'en finir.

La première consiste à le rejeter en considérant que nous ne sommes pas dans une société surveillée par le *Big brother*. Mais il en est une autre et je ne vous cache pas que c'est ma thèse : ce mythe a disparu puisqu'il est devenu une réalité entre-temps.

En effet, je crois que fondamentalement nous vivons dans une société de surveillance. La vraie question que je me pose est donc de savoir comment on peut essayer de vivre dans cette société tout en exerçant une espèce d'auto vigilance. Il y a ceux qui se demandent comment éviter d'entrer dans cette société et ceux qui se demandent comment y vivre. D'une certaine façon, ils se rejoignent car tous ceux qui ont des responsabilités dans ce domaine se demandent comment assurer le progrès économique et social et en même temps assurer le mieux possible la préservation des libertés fondamentales.
Dans le débat d'aujourd'hui, la CNIL n'est qu'un acteur. Je l'espère un acteur important. Mais elle est d'abord là pour écouter. La vocation de la CNIL n'est pas d'être une juridiction, n'est pas d'être une association, ni d'être le législateur, ni l'exécutif, ni une société commerciale. Et pourtant, la vocation d'une autorité administrative comme la nôtre, c'est tout de même d'exercer un certain de nombre de tâches qui ressortissent à chacun des acteurs que je viens d'évoquer. C'est ce qui lui

donne à la fois sa spécificité et son originalité. Peut-être que parfois cela trouble un peu son image. C'est pourquoi après un an et demi de présidence de la CNIL, je crois bon de rappeler le positionnement singulier et la sensibilité particulière que doit avoir la CNIL vis-à-vis des problématiques qui nous intéressent aujourd'hui.

Comment cela se traduit-il ? Premièrement, la CNIL doit toujours tenter de se placer dans le futur. Son rôle n'est pas d'être un organe qui contrôle, vérifie la légalité en tant que telle seulement. Ce n'est pas non plus, on l'a dit déjà, un organe qui est à l'origine des textes. La CNIL doit s'efforcer de se placer un peu plus loin dans le futur et essayer d'imaginer les dérives potentielles en germe dans les actions ou les textes pour proposer en amont, par exemple dans le débat parlementaire, des solutions pour faire en sorte que le champ des garanties soit le plus précis et le plus étendu possible.

La CNIL ne se prononce pas seulement en légalité pure et encore moins en opportunité. Lorsque l'on a expliqué à la CNIL quelle était la finalité d'un projet, elle se prononce en termes de proportionnalité. Mais tous les juristes qui sont présents dans la salle savent à quel point la notion même de proportionnalité emprunte à la fois au concept de légalité et au concept d'opportunité. C'est aussi une des raisons qui font que les positions de la CNIL sont parfois mal comprises : parce qu'on ne l'attend pas là où elle doit se trouver en vertu des lois fondatrices. Notre commission se voit confiée, surtout depuis la loi de 2004, des tâches extrêmement lourdes.

La première est de mettre en route cette nouvelle loi et de développer un effort considérable en matière de pédagogie, d'information, de formation et de développement des correspondants informatique et libertés. Ceux-ci constituent en effet un nouveau mécanisme dont nous attendons énormément puisqu'il doivent s'implanter dans l'ensemble des entreprises, des administrations ou des collectivités locales. Nous devons également renforcer de façon très significative notre politique de contrôle puisque c'est le corollaire de l'allègement des formalités préalables. À défaut, c'est le niveau de protection des données personnelles qui serait en cause.

Deuxièmement la CNIL a en charge l'analyse des textes législatifs et réglementaires. Je pense, par exemple, au développement de l'administration électronique, au dossier médical personnel et à tous les textes liés au développement d'impératifs de sécurité pour les raisons que chacun connaît.

Enfin, la CNIL se trouve au cœur de problématiques fondamentales pour notre société. Je citerai la biométrie, la géolocalisation, la vidéosurveillance, les lignes éthiques, les fichiers positifs sur l'endettement des particuliers, les fichiers d'infractions mais aussi la relation transatlantique (États-Unis / Europe) vis-vis du champ de la protection des données.

C'est une commission nouvelle qui vient aujourd'hui participer à ce colloque et qui attend beaucoup des échanges qui vont suivre. Si nous avons une vocation, nous avons aussi, si j'ose dire, un « destin ». Notre destin est d'être systématiquement au milieu d'un champ croisé de critiques, d'une « interconnexion » de critiques. Comment sortir d'un débat quand on sait que soit les internautes, soit les sociétés

d'édition musicale seront mécontents ? Je pourrais multiplier les exemples. On le voit, notre situation est toujours difficile et complexe. Nous ne pourrons jamais, et ce n'est pas notre rôle, plaire à tout le monde. Notre rôle, est à un moment donné, de proposer un équilibre fondamental qui nous paraisse acceptable par la société. Il nous faut faire preuve de stoïcisme pour affronter les « avanies » que suscitent nos positons présentes tout en faisant preuve de clairvoyance et tenter de deviner le futur. Nous venons ici devant vous pour essayer de mieux éclairer notre chemin.

Qu'il me soit également permis de remercier Christophe PALLEZ, secrétaire général, Marie GEORGES ainsi qu'Elsa TROCHET-MACÉ qui ont contribué à l'organisation de ce colloque.

2. Allocution de M. Dominique CHAGNOLLAUD Professeur à l'Université de Paris II (Panthéon-Assas), Vice-président du Conseil supérieur de la recherche et de la technologie (CSRT)

C'est un grand honneur pour notre université de droit, que la CNIL ait bien voulu nous associer à ce colloque. Son thème est en effet au cœur des préoccupations des juristes, y compris des constitutionnalistes dans la mesure où il embrasse des questions intéressant directement les droits et libertés fondamentaux. Vous savez que notre université est à la pointe des études françaises et comparatives sur ces questions. Je vous remercie donc encore une fois, monsieur le président de la CNIL, de nous avoir associé à cette rencontre.

Je voudrais aussi remercier le président PONCELET, qui a souvent appuyé nos initiatives et je sais l'attachement de la deuxième chambre aux libertés. Je remercie tout particulièrement M. Alain MÉART, directeur de cabinet de M. PONCELET. Enfin, je remercie M. Dominique WOLTON, qui a contribué par sa réflexion à ce colloque, ainsi que M. PALLEZ, secrétaire général de la CNIL. Tous ensemble, nous avons construit ce projet qui je l'espère sera réussi.

Je suis pour ma part quelque peu néophyte dans les matières qui nous intéressent aujourd'hui puisque je ne m'y suis intéressé qu'indirectement, par le biais des droits et libertés fondamentaux. Mais en lisant, en relisant et en écrivant un certain nombre de choses, en compulsant la littérature étrangère et française, j'ai été frappé de quelques points très simples, que, devant ce public de spécialistes, j'ai peine à rappeler. Il s'agit avant tout de l'interdépendance entre trois facteurs : d'abord la norme ou l'édiction de la norme, puis la fabrication implicite des normes que peut produire la technologie, et enfin le marché. Je dirais, pour être bref, comme l'avait souligné un de mes collègues il y a quelques années, qu'il s'agit précisément d'analyser cette interaction entre ces trois secteurs : la norme juridique, la technologie qui produit ses propres normes, et le marché.

C'est à partir de là que le juriste que je suis, politologue aussi à ses heures, est extrêmement humble : je suis pleinement conscient de la difficulté qu'il y a à

encadrer des phénomènes qui, pour certains, sont absolument effrayants, dès lors que l'on ne dispose pas d'une capacité de contrôle et de coopération avec les acteurs du secteur, ni d'une bonne connaissance des technologies qui sont en jeu, en tous cas en Europe, puisque le modèle américain est différent.

Je m'arrêterai là en vous disant qu'au fond, en tant que juriste, il m'est apparu central d'essayer de comprendre comment ces trois secteurs – le secteur juridique, le secteur technologique, le marché – pouvaient interagir.
L'enjeu de ces questions ne doit pas être sous estimé, il s'agit tout de même, sans exagérer, non seulement la protection de la vie privée mais aussi la dignité humaine. Nous aurions donc aussi pu, à ce propos, convier à ce colloque des anthropologues, et nous essayer à l'anthropologie juridique. Ces questions peuvent porter atteinte à la dignité même de l'homme et à ce titre, elles nécessitent d'être réexaminées.

En tous états de cause, en organisant ce colloque, nous avons cherché à y associer des personnalités d'horizons très divers : juristes, politologues, magistrats, sociologues, industriels. Je les remercie pour leur présence et comme le disais quelqu'un que j'aime beaucoup : « c'est à ce carrefour de la pensée que nous vous invitons donc maintenant ». Je vous remercie.

B. L'HOMO INFORMATICUS : RÉALITÉS ET TENDANCES

14h30-18h00
Présidence M. Alex TÜRK

1. Sécurité : l'exemple de l'identification biométrique

M. Bernard DIDIER
Directeur Scientifique et du Développement des Affaires – Division Sécurité – Sagem Défense Sécurité – groupe SAFRAN

M. Philippe LEMOINE
Président directeur général de LaSer et de Cofinoga, membre de la CNIL

M. Bernard DIDIER

Directeur Scientifique et du Développement des Affaires – Division Sécurité – Sagem Défense Sécurité – groupe SAFRAN

En introduction, de courtes présentations de films présentent le développement de la biométrie dans différents pays et pour différents usages :

Afrique du Sud : plus de deux millions de pensions sont distribuées dans le bush et des villages reculés. En présence d'une population en partie analphabète, la biométrie se substitue à l'usage de code de sécurité personnel.

Mauritanie : la biométrie est utilisée dans le désert pour aider à la constitution d'un état civil et d'une liste électorale sans doublon.

France : plus de 130.000 personnes utilisent régulièrement des contrôles d'accès à empreinte digitale, avec des badges sans contact, pour accéder aux zones sensibles des aéroports d'Orly et de Charles de Gaulle.

Australie : le projet Smartgate de contrôle du passage aux frontières avec des passeports à lecture sans contact et reconnaissance automatique du visage.

France : le projet Pégase de contrôle de passage aux frontières par reconnaissance de l'empreinte digitale.

Angleterre : le projet Iris de contrôle de passage aux frontières par reconnaissance de l'iris.

France : l'exemple du contrôle des passagers, à l'aide de reconnaissance automatique d'empreintes digitales, à l'enregistrement et lors de l'embarquement dans des avions.

Allemagne : des paiements par empreinte digitale dans un supermarché suppriment l'usage de cartes bancaires ou de chèques.

Un rappel sur les fondements de la biométrie, dont l'objectif est d'établir un lien entre la représentation immatérielle d'un monde et le monde vivant, permet de comprendre la complémentarité de cette technique avec les autres techniques d'authentification. Il est ensuite donné une définition de la biométrie, qui pour la première fois, étend le concept d'identification et d'authentification à celui d'un **groupe de personnes**. Enfin, sont rappelés les trois critères de choix d'une biométrie : l'unicité, l'universalité et l'immuabilité.

Ces critères permettent d'apprécier subjectivement les performances que l'on peut attendre de la reconnaissance du visage, de l'empreinte, de l'iris et de techniques moins performantes telles que la reconnaissance des longueurs des doigts ou de la signature. L'appréciation objective est introduite au travers des ratios classiques de faux rejets et de fausses acceptations présentant l'arbitrage incontournable entre confort et sécurité.

Ce volet technique est ensuite complété par une présentation des marchés :

Une première segmentation présente un marché **gouvernemental**, acteur historique sur le segment de marché mature de la Police et acteur de développement d'un segment de marché de gestion de droits **civils** (passeports, cartes d'identité…), un marché des **entreprises** en début de développement et un marché des **particuliers** qui connaît une amorce de croissance particulièrement rapide au travers des équipements en capteur d'empreintes d'ordinateurs portables, de téléphones mobiles ou d'assistants personnels.

Une analyse, vue sous un angle plus technologique, complète la précédente. Ainsi le marché des droits civils s'adresse à quelques **Intégrateurs** aptes à développer des solutions d'ampleur étatique, ce marché des systèmes policiers est tenu principalement par quatre **Systémiers** maîtres de leur technologie biométrique, le marché des entreprises concerne plus particulièrement des **Equipementiers** biométriques au nombre de quelques centaines, enfin le marché des particuliers est aujourd'hui couvert par quelques vendeurs OEM de **Composants** de lecture d'empreintes.

Pour conclure cet exposé sont présentés les grandes tendances en matière de biométrie :

Historiques : la demande biométrique à usage civil n'est pas née de l'après 11 septembre 2001, ce marché a pris corps au début des années 1990 et son chiffre d'affaires est devenu supérieur à celui du marché policier en 2004. Sur le plan

technique, l'empreinte digitale qui a bénéficié d'investissements réguliers depuis plusieurs décennies reste de loin la technologie la plus utilisée.

Géopolitiques : l'après 11 septembre a suscité la mise en place d'une interopérabilité mondiale et transformé la biométrie en technologie de souveraineté. Dans un tel contexte, certains États ont retardé leurs décisions d'équipements. L'industrie américaine de la biométrie devrait tirer quelques avantages : d'un marché intérieur important, de la politique de protection des frontières et des budgets de recherches du gouvernement américain. Face à la montée en puissance d'une demande biométrique, l'Asie plus que l'Europe semble pouvoir concurrencer un tel développement.

Techniques : l'empreinte restera la technologie de référence, mais la technologie de reconnaissance du visage devrait être celle qui connaîtra les améliorations les plus importantes, l'iris devrait définitivement avoir résolu ses problèmes de facilité d'usage et devrait devenir une technique confortable et performante. Les gouvernements devraient utiliser assez rapidement des technologies en combinaison pour améliorer les performances et rendre plus difficile la fraude. Un effort particulier sera fait sur les mécanismes de détection des attaques par leurre et devrait amener à reconsidérer le concept de biométrie à trace. Enfin, dans un proche avenir l'existence de mécanismes permettant de déduire des codes stables à partir de l'analyse intrinsèque d'un élément biométrique pourrait modifier profondément l'univers de la biométrie.

Usages : des populations importantes vont découvrir la biométrie au travers des contrôles de passage aux frontières, la mise en place de cartes d'identité biométriques devrait suivre dans un second temps. Le relais d'usage devrait se faire, via des emplois personnels, au travers d'objets mobiles (téléphone, PDA, ordinateurs portables). Les entreprises devraient utiliser la biométrie pour sécuriser leurs systèmes d'informations et exiger ultérieurement une convergence avec la sécurité physique. Enfin les banques pourraient être amenées à se substituer à des opérateurs indépendants qui auront été des précurseurs de moyens de paiements biométriques.

Economiques : sauf accidents dus à des promesses déraisonnables de développements de certains acteurs - qui pourraient provoquer un effondrement des valeurs de société, ternir l'usage de la biométrie et ralentir le développement du marché – la valeur des sociétés de biométrie devrait continuer à s'appuyer sur des ratios exceptionnels avant de retrouver, avec la consolidation des acteurs, un contexte plus classique.

M. Philippe LEMOINE

Président directeur général de LaSer et de Cofinoga, membre de la CNIL

Le problème de l'identification biométrique est abordé sous trois angles par la loi du 6 Janvier1978 modifiée par la loi du 6 Août 2004 :

- Sous l'angle d'abord de la protection de l'identité humaine : le principe posé par l'article 1 de la loi est que l'informatique ne doit en aucun cas porter atteinte à l'identité humaine. C'est même le premier des critères : « 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. »

- Sous l'angle juridique ensuite des conditions de licéité des traitements de données à caractère personnel : le principe posé par l'article 8 de la loi est l'interdiction de collecter ou de traiter certaines catégories de données. En tête de ces données souvent qualifiées de données sensibles se trouvent toutes les données qui pourraient faire apparaître directement ou indirectement les origines raciales ou ethnique des personnes, parmi lesquelles figurent évidemment les données biométriques. Les autres composantes de ce que la loi considère en quelque sorte comme le noyau dur de l'identité humaine sont « les opinions et les appartenances (politiques, philosophiques, religieuses, syndicales) ». Y ont été ajoutées les données relatives à la santé et à la vie sexuelle, qui peuvent avoir de plus lointains rapports avec la biométrie.

- Sous l'angle pratique enfin des formalismes auxquels sont soumis les traitements comportant des données biométriques nécessaires au contrôle de l'identité humaine : ces traitements échappent au régime déclaratif du droit commun pour relever de procédures d'autorisation. Les procédures ne sont toutefois pas les mêmes, selon que les traitements sont mis en œuvre par des entreprises ou par l'État, qu'ils relèvent d'un usage répandu ou qu'ils concernent la sûreté de l'État, la Défense et la sécurité publique.

Ces trois points de vue philosophique, juridique, pratique ont une importance particulière au regard d'un **double choc**. **Le choc technologique d'abord** que constitue le progrès très rapide des technologies biométriques, qu'il s'agisse de la numérisation de certaines caractéristiques que l'on savait saisir depuis longtemps (photos, empreintes digitales, empreintes vocales), de détection de nouveaux moyens biologiques (iris, ADN, odeur etc…), de perfectionnement de logiciels de reconnaissance automatique des formes, de capacité de moins en moins onéreuses de stockage de masse, de rapidité de balayage des grandes bases, de données, d'actualisation des composants électroniques situés sur des cartes ou des documents, de lecture à distance d'implants électroniques ou directement de composants biologiques. **Le deuxième choc est de caractère sociétal voire civilisationnel** avec la montée de toutes les questions relatives aux enjeux de sécurité, au premier rang desquels figure le terrorisme international dont l'universalité de la menace est telle que certains considèrent les démocraties comme engagées dans une sorte de 3ème guerre mondiale.

La mise en perspective est donc celle de trois questions fondamentales :

- l'interrogation philosophique : qu'est-ce que l'identité humaine et en quoi est-elle en jeu avec la biométrie ?

- l'interrogation juridique : qu'est-ce que l'identification biométrique a-t-elle de particulier et en quoi le traitement par une machine de certaines données est-il plus sensible que celui par exemple qui s'opère dans un cerveau humain ?

- l'interrogation pratique et politique : les procédures et les formalismes qui ont été définis sont-ils efficaces ? Assurent-ils un bon équilibre dans un État moderne de Droit ?

1. Qu'est-ce que l'identité humaine ?

Il est bien évidemment hors de propos de vouloir ici, dans ce Colloque, répondre à une telle question. Il n'est même pas pensable de vouloir faire le tour de ses différentes dimensions.
Il est par contre utile de rappeler le contexte dans lequel la problématique « Informatique et Liberté » s'est constituée en France et dans les démocraties européennes, afin de comprendre la portée conférée par la loi à cette notion d'identité humaine. Ce contexte est triple :

- Un débat est en cours au milieu des années 70 sur le numéro d'identification des Français et sur le système SAFARI. Celui-ci entend généraliser dans l'informatique le numéro de Sécurité Sociale créé en France en 1942 afin de contrôler les populations dans le cadre de l'Occupation et de détecter les personnes survivant sous une fausse identité. Un ensemble de questions liées à la seconde guerre mondiale remontent alors à la surface et justifient que l'on se réfère à l'identité humaine : les questions fondamentales soulevées par le totalitarisme et formulées notamment par Alfred KOESTLER, par Anna HARENDT et par Georges ORWELL ; les questions plus spécifiques ayant fait irruption dans le champ philosophique et soulevées par le nazisme, par le projet de solution finale et par les camps de concentration et d'extermination.

- Ce débat des années 70 reprend ainsi des questions des années 40 mais il ré-interroge également une expérience historique longue, celle de l'histoire humaine qui établit que l'humanité se pense elle-même à travers certains interdits concernant les représentations. La Bible enseigne que l'on ne compte pas les hommes comme des moutons. De nombreuses religions interdisent la représentation corporelle de Dieu et mettent en garde contre le risque d'idolâtrer l'image de l'homme, dans les représentations de son visage ou de son corps. Les anthropologues illustrent l'universalité des conduites liées au caractère sacré de la mort et à la non sacralisation des représentations de la vie. Dans « Lascaux ou la naissance de l'Art », Georges BATAILLE montre comment l'homme préhistorique représente parfaitement les bisons et les aurochs mais qu'il s'interdit de se représenter lui-même et que c'est par cet interdit qu'il parvient à la conscience même de ce qu'est l'humanité.

- Une troisième dimension du débat des années 70 concerne les sciences sociales et l'opposition entre anthropologues et sociologues dans l'approche du concept sociétal d'identité. Un séminaire animé par Claude LEVY-STRAUSS au

Collège de France en 1978 porte précisément sur cette opposition. Les anthropologues considèrent que l'identité relève de l'ordre du Même, des invariants qui caractérisent une société et, donc pour chaque individu de ce qui appartient à la tradition, de ce qui est transmis et hérité. Les sociologues considèrent au contraire cette définition de l'identité comme pré-sociologique, représentative d'une société holiste ou chacun se définit par rapport au Tout, mais sans pertinence par rapport à une société individualiste où la société se constitue par les interactions et les projets noués entre les personnes. Pour celles-ci, l'identité relève de moins en moins de l'héritage et de plus en plus d'un projet personnel dont chacun veut être l'architecte. C'est même ainsi que l'on peut définir la modernité sous ses différentes acceptions et plus encore les formes nouvelles de modernité qui apparaissent à compter des années 70, en rupture avec la modernité classique. Depuis DERRIDA, LYOTARD, Ulrich BECK et Anthony GIDDENS, la notion de personne se libérant d'une définition unitaire de l'identité institutionnelle et construisant une trajectoire spécifique à partir de l'éclatement des identités multiples et de l'acceptation de la différence, est au cœur du projet émergent de nouvelles modernités.

2. On en vient à la seconde grande question : en quoi les données biométriques interfèrent-elles avec ces enjeux et en quoi la mise en œuvre informatisée des procédures d'identification constitue-t-elle une menace spécifique ?

Les quatre horizons temporels que nous venons de rappeler caractérisent bien les quatre catégories d'enjeux qui concernent l'identité humaine : l'enjeu immédiat des années 70 c'est le projet SAFARI et **l'informatisation de l'identité administrative.** L'enjeu des années 40 qui remonte ainsi à la surface c'est celui des dangers de l'État totalitaire et en particulier ceux **du contrôle centralisé des comportements individuels et ceux de la discrimination raciale.** L'enjeu d'histoire longue qui a été ré-évoqué, c'est celui de l'**identité humaine**, ce qui fait qu'un homme est un sujet et non un objet, un corps parlant et pensant, distinct d'un animal, un sujet vivant mais qui ne se prend pas pour Dieu ou un sur-homme. L'enjeu prospectif, celui d'un futur émergent dès les années 70, plus nettement affirmé aujourd'hui, c'est celui d'une **modernité tiraillée** par la crise des ordres et des institutions mais relayant malgré tout une demande de sécurité, tandis que les personnes font de la construction de soi un enjeu majeur, bien plus citoyen que simplement égoïste, en rupture avec les identités héritées, immuables, affiliées ou assignées.

Ces quatre enjeux sont tous démultipliés par la biométrie. La biométrie, c'est en effet l'évacuation de l'ambiguïté que recèlent les différentes dénominations patronymiques et c'est toute la problématique **du risque de contrôle totalitaire.** C'est par définition le règne des données bio-corporelles et c'est la crainte d'une dérive vers les idéologies de la **discrimination raciale.** C'est la multiplication des facettes du corps vues, analysées et commentées, avec tous les dangers d'une **banalisation de l'idée même d'humain.** C'est la recherche de critères toujours plus immuables et intangibles, au moment où la **revendication démocratique** prend la forme d'une aspiration à l'auto-production de soi.

Aussi est-ce par rapport à ces quatre enjeux fondamentaux et à leur combinatoire que la CNIL élabore depuis plusieurs années une doctrine et une pratique de l'identification biométrique :

- Face au risque de contrôle totalitaire, la CNIL essaye de **dissocier le moyen d'authentification** de l'identité personnelle que forment des données biométriques stockées sur une puce **et le moyen de contrôle généralisé** que constitueraient ces mêmes données reprises dans une base de données centrale. La distinction est loin d'être inutile aujourd'hui, même si les perspectives technologiques des réseaux et du P-2-P effaceront progressivement cette distinction au profit de notions de bases de données virtuelles éclatées entre de multiples supports de plus en plus communicants. Aussi cette première distinction, se double-t-elle aujourd'hui d'une distinction entre données stockées sur une puce qui ne peut être lue que par un contact physique, maîtrisé humainement, et sur un composant de type RFID qui peut être lu à distance.

- Face au danger de la discrimination, la CNIL s'attache au principe fondamental qu'est pour elle le **principe de finalité.** Une application est autorisée dans un certain but et des données collectées dans un but ne peuvent être utilisées qu'à cette fin. Ce principe essentiel doit se doubler de trois précautions. D'abord des précautions en cas de sortie possible du régime d'État de Droit : il peut être ainsi imaginé que la CNIL se réserve le droit de détruire tel ou tel système d'information autorisé en temps normal. Ensuite en cas de détournement des finalités : cela suppose un arsenal de moyens de sanctions dont la CNIL dispose et un arsenal de moyens de contrôle dont la CNIL dispose juridiquement mais pas financièrement. Enfin, un principe d'exigence et d'intelligence froide doit présider à l'examen des finalités décrites dans les demandes d'autorisation qui peuvent être présentées dans des contextes très chauds et très émotionnel d'attentats, de massacres, de violence. On y reviendra.

- Face à la multiplication des représentations du corps et à la banalisation possible de la vie humaine, la CNIL construit une jurisprudence fondée sur la notion de **« traces »**. Dès lors que les capteurs électroniques se multiplient, toutes les données biométriques peuvent laisser derrière elles des traces. On considère ainsi que quelqu'un qui travaille à Manhattan laisse derrière lui chaque jour 75 images de son visage sur les systèmes de vidéosurveillance. Les Londoniens dépassent 200 dès lors qu'ils sont au volant d'une voiture. Il n'empêche que certaines mesures ont besoin d'un capteur pour être transformées en traces : c'est le cas de la photo ou de l'analyse de l'iris par exemple. Par contre, l'ADN et l'empreinte digitale laissent spontanément des traces bio-chimiques que l'on peut décrypter a posteriori. La CNIL est donc plus réservée sur ces outils.

- Face à la rigidification d'une identité biométrique devenue immuable, la CNIL veille à ce que tous les systèmes soient mis en place pour des **durées définies et légitimes**, conformes à la finalité spécifique d'un traitement. La question est importante car la plupart des marqueurs biométriques sont des identifiants éternels parfaits : ils sont uniques, avec des risques de confusion

infinitésimaux ; ils ne varient pas dans le temps. La photographie d'un visage est certes de moins en moins juste avec le temps. Mais un article récent rappelait que la reconnaissance automatique du visage avait été classée technologie ultra-fiable, alors qu'au moment des attentats de septembre 2001, le taux de réussite d'un logiciel comparant une photo et une base d'images importantes n'était que de 60%. Ce taux dépasse aujourd'hui 90% et des recherches fondées sur un traitement 3D de l'image visent à maintenir un taux satisfaisant de reconnaissance malgré un maquillage ou malgré le vieillissement.

3. Il y a aussi des marges de manœuvre dont la CNIL se saisit et c'est son rôle de le faire. Mais chacun peut en voir les limites. **D'où l'interrogation pratique et politique : les procédures et les formalismes définis sont-ils efficaces ? Assurent-ils un bon équilibre entre les impératifs de sécurité et de Libertés ?**

Dans un article sur l'identité informatisée publié en 1980, nous écrivions que le risque majeur de l'informatique allait consister en un achèvement du mouvement séculaire de quadrillage de l'identité humaine par l'identité administrative et en un enracinement brusque et direct de cette identité administrative dans une identité biologique et corporelle. Autrement dit fromage et dessert ! Les dangers de la glaciation et de la réification de l'humain tels que les envisagèrent FOUCAULT et le structuralisme dans les années 70, celui d'un homme pris en tenaille entre un pouvoir et un savoir de plus en plus imbriqués. Les dangers de la désagrégation des légitimités institutionnelles et des mécanismes d'ordre, de la contamination généralisée de l'instabilité et du doute qui sont propres au savoir. Les deux risques se conjuguent pour mettre en scène, dans un contexte de communication généralisée, la spirale folle de personnes à la recherche de leurs identités et de sociétés en quête de leur sécurité, dans un tourbillon où les uns et les autres se répondent à travers des technologies de plus en plus sophistiquées, mais de moins en moins maîtrisées, d'identification, de simulation, de prévision et de prévention.

Internet joue un rôle d'accélérateur dans ce tourbillon. L'attractivité du nouvel espace public que constitue le Web est telle que beaucoup d'applications qui s'y développent ont des impératifs de sécurité inconciliables avec la mentalité libertaire qui y règne. Beaucoup d'applications transactionnelles auraient plus leur place sur des réseaux privatifs utilisant Internet que sur le Web. Mais ce n'est pas ce qui se passe et des solutions de plus en plus sophistiquées se développent, souvent fondées sur la biométrie, pour tenter de concilier l'ouverture du Web et le besoin de sécurité.

Mais ce qui accélère vraiment les dérèglements de la spirale, c'est le couple Internet/terrorisme. Les démocraties utilisent les technologies d'information pour traquer le terrorisme ; les terroristes utilisent Internet pour s'organiser. Il s'agit en quelque sorte de deux frères ennemis. On dit parfois qu'Internet est ATAWAD : any time, anywhere, any device. Tout le temps, partout, avec n'importe quel média. Est-ce que cela ne serait pas aussi le slogan de la terreur, ATAWAD ? Elle peut frapper partout, à toute heure, avec n'importe quelle arme.

Ces mécanismes contribuent à créer des contextes passionnels où le risque c'est que plus personne ne contrôle ce qui se passe. Les ministres ne contrôlent plus toujours leurs services. Les chefs de Gouvernement, leurs ministres. Le Parlement, les Gouvernements. Or il est indispensable de contrôler au sens de vérifier, analyser en profondeur, lutter contre la désinformation, distinguer, dans un contexte où se mêlent paranoïa technologique et paranoïa sécuritaire.

Vérifier : des faits peuvent être inexistants, comme l'illustre par exemple l'élaboration de règles de police administrative dans l'affaire montée de toutes pièces du bagagiste d'Orly ou l'incroyable contraste entre les faux repérages d'usines atomiques en Irak par les services secrets et l'impression que peut avoir le grand public de voir la terre entière à travers le logiciel Google Earth. Analyser en profondeur : j'ai déjà raconté comment, alors Commissaire du Gouvernement auprès de la CNIL, j'avais détecté une mention « type juif » dans la nomenclature du système VAT (violence/attentats/terrorisme) conçu par un Ministre de Gauche à la suite de l'attentat de la Rue des Rosiers ! Lutter contre la désinformation : le Président BUSH père se méfiait tellement des dossiers de la CIA qu'il avait dirigée, qu'il se dit que, devenu Président, il avait créé une équipe B, chargée de contre instruire les dossiers, à laquelle appartenait Paul WOLFOWITZ. Distinguer : la CNIL s'attache en permanence à maintenir une distinction entre police judiciaire et police administrative, alors que les textes sécuritaires tendent à gommer cette distinction, créant des situations incroyables où des jeunes qui ont fumé un joint se retrouvent mêlés à des suspects du terrorisme et barrés, même pour un emploi d'agent de sécurité dans un aéroport !

Sur tous ces sujets, la CNIL dispose des compétences humaines et techniques pour faire face. Peut-être devrait-elle mieux faire savoir et la gravité des enjeux et les positions qu'elle soutient ? Une limite est toutefois le cas, de plus en plus fréquent, où un système sécuritaire est créé par la loi. Alors que la hiérarchie des normes donnait une grande efficacité à la loi Informatique et Libertés face à des systèmes d'information créés par décret ou par arrêté, le contexte actuel amène de plus en plus souvent les politiques à recourir à la loi. Les menaces que la biométrie peut faire courir à notre civilisation, couplées aux enjeux inéluctables de la lutte contre le terrorisme devraient conduire à agir sur ce point. Il faudrait faire en sorte qu'en matière biométrique notamment, la CNIL intervienne sur les projets ou les propositions de loi et qu'elle soit peut-être à la disposition du Conseil Constitutionnel pour examiner la constitutionnalité de telle ou telle disposition arrêtée par le Parlement.

Ce dernier point, comme tout ce qui précède d'ailleurs, est un point de vue personnel, celui de quelqu'un qui croit réellement à l'importance de ces enjeux. Il n'engage en rien l'institution à laquelle j'appartiens.

2. Commerce : la personnalisation des relations

M. Christophe POUPINEL
Président-directeur général de ChateauOnline

M. Serge GAUTHRONET
Consultant – Président du Directoire ARETE

M. Christophe POUPINEL
Président-directeur général de ChateauOnline

Mon propos va être bien plus terre à terre, je vais vous parler de vin, nous allons redescendre dans les vignes… Mais plus exactement, on m'a demandé de représenter ici, un certain type de société qui utilisaient donc les données personnelles, des sociétés d'Internet, et à l'intérieur des sociétés d'Internet, les sociétés qui font du commerce, qui vendent des choses.
En un mot, qui nous sommes, ce qui vous permettra de mettre en perspective mon discours et moi de faire un peu de publicité, si vous voulez acheter du vin, maintenant vous savez où le faire ! ChateauOnline est la société leader de vente de vin sur Internet, donc 50% de notre activité en France, 50% en Europe. 90% de ce chiffre est fait en vente aux particuliers, et donc, nous avons dans nos bases de données, dont on va parler, 500 000 abonnés à nos newsletters – donc des particuliers qui ont cliqué ou qui ont appuyé sur un petit bouton qui dit « je souhaite recevoir la lettre des grands vins », « la lettre des enchères sur le vin », « la lettre éditoriale sur le vin », voilà les différentes lettres d'information – dont à peu près 60 000 clients.

Les trois questions auxquelles je vais essayer de répondre : de façon très terre à terre, vous montrer le type de données que l'on recueille, comment nous les recueillons ; deuxième question, qu'est-ce que l'on en fait ; et , mon point de vue, est-ce que c'est une liberté ou une servitude pour le consommateur.

Premier point : quel type de données consommateur et comment les recueillir ?
Nous avons deux types d'informations : des données historiques de comportement d'achat et des données déclaratives. Donc les données historiques, pour ceux qui viennent de l'Industrie ou qui sont familier avec l'Industrie et la vente par correspondance, cela paraît totalement évident, mais comme vous venez d'univers différents, je crois que c'est important de le rappeler.
Première chose très simple : nous conservons l'historique des commandes de chaque client. ChateauOnline a été créé dès 98, pour faire de l'Internet, donc dès le premier jour de notre activité, nous savions que c'était le cœur de notre métier et donc, nous avons mis en place tout un système de bases de données pour pouvoir recueillir ce type d'informations. Nous savons ce que chacun de nos clients a acheté et quand il a

passé cette commande : c'est la base de la Vente Par Correspondance, ce qui est un peu nouveau c'est que l'informatique s'est développé depuis ces dernières années, il y a eu une sorte d'accélération, alors qu'il y a pas mal de société de VPC qui ont 50 ans et dont les bases de données n'étaient pas très bien structurées pour pouvoir utiliser de façon aussi efficace que les bases de données que d'autres sociétés comme la nôtre ont pu mettre en place immédiatement. Parce que c'est une chose d'avoir les bases de données, c'en est une autre de pouvoir les utiliser.

Deuxième type de données, ce sont les données déclaratives : on pose un certain nombre de questions à nos clients, bien sûr leur âge, et des informations sur leurs goûts, leurs habitudes. Comment les recueillir ? Les données historiques de comportement d'achat, le client qui achète sur chateauOnline, comme sur beaucoup d'autres sites e-commerce, dispose d'un compte client, lui permettant de ne pas re-saisir son adresse, son numéro de téléphone, de consulter l'historique de ses commandes, de suivre la livraison de ses commandes en cours, et bien d'autres fonctionnalités, comme justement la gestion de ses abonnements aux newsletters, la gestion et la possibilité d'avoir plusieurs adresses de livraison et des cadeaux récurrents… Si vous avez passé des commandes sur le net, vous connaissez cela très bien. Juste une information : nous ne conservons pas les données bancaires, certains sites le font, nous ne le faisons pas. Si le client utilise son compte, toutes ses commandes lui sont rattachées et il n'a « rien à faire de plus » qu'utiliser son compte. Rien n'empêche un client d'ouvrir un compte différent : en général, ce n'est pas volontaire de la part du client, c'est plutôt qu'il a oublié son mot de passe, et donc il va recréer un compte, et donc il est possible d'avoir un même client qui va avoir plusieurs comptes. On peut, comme on dit, dédupliquer les comptes sur, par exemple, le nom de famille et scinder ces comptes, ce qui normalement est un travail que toute bonne société doit faire régulièrement. Les données déclaratives sont communiquées à travers divers questionnaires en ligne, à certains points de contact avec le client, je vais vous en montrer un, qui est très simple, c'est un questionnaire sur le profil d'amateur de vin, que l'on pose à différents moments : quand vous venez d'ouvrir votre compte, on vous pose ces questions, vous n'êtes évidemment pas obligé d'y répondre ; lorsque vous venez de passer une commande, dans les envois d'e-mail de confirmation de commande, on va vous renvoyer des liens vers ces questionnaires. Nous avons toute une batterie de moyens pour savoir si nos clients ont répondu à ce questionnaire ou d'autres, et continuer à poser ces questions, pour justement remplir nos bases de données.

Petits exemples de questions :

ce que vous aimez, vos régions de prédilection…
Là c'est une segmentation régionale, donc on demande à nos clients s'ils aiment bien, s'ils ne connaissent pas très bien mais qu'ils aimeraient découvrir, s'ils ne sont pas du tout intéressés. Vous pouvez imaginer ce qu'on en fait après…

Une question amusante :
votre niveau en vin est : nul et le restera ; et c'est exactement phrasé de cette façon là ; et il y a assez peu de Français qui répondent oui à cette question là, beaucoup plus d'Anglais et d'Allemands.

Il y a des questions amusantes comme les questions entre le déclaratif et la réalité : lorsque vous demandez au client combien il dépense par bouteilles ou même dans l'année, il y a toujours une surestimation de ce que l'on fait vraiment, alors ils vont vous dire qu'ils achètent des bouteilles à 20 ou 30€ et après vous voyez dans leurs données historiques, qu' ils achètent plutôt à 10-15€.
D'autres questions assez typiques sur le degré de satisfaction sur ChateauOnline sont posées.

Deuxième point : que fait-on de ces données ? Le *scoring*.
Encore une fois pour les spécialistes de la VPC et du commerce, ce que je vais dire, vous le connaissez par cœur, pour les autres, ça vaut le coup d'être explicité. Vous avez sans doute entendu parler du *scoring* : le *scoring* généralement se fait sur de nouveaux clients. Le problème, quand vous avez un nouveau client, une première commande, c'est que vous ne connaissez pas le potentiel de ce client. Une des utilisations du scoring, c'est de pouvoir déterminer ou plutôt d'évaluer le potentiel de ce client. Donc le client passe une première commande, donc on a des données sur une première commande. S'il a répondu à certains questionnaires, nous avons aussi des données déclaratives. Ce que l'on fait, c'est comparer les données de la première commande et les données déclaratives au profil d'un « bon client ». On sait statistiquement ce qu'est la première commande d'un « bon client », puisqu'on a huit ans d'histoire et d'historique de commandes. On a dans la base, le profil type d'une bonne première commande, c'est-à-dire celui d'une commande d'un client qui va, après, en passer d'autres. C'est un programme statistique qui nous permet de « comparer » cette « première commande » à la « bonne » première commande-type et d'attribuer donc un score à ce nouveau client : plus le score est élevé, plus ce nouveau client a du potentiel. L'idée est évidemment d'investir plus de temps et d'argent sur le bon client.

M. Serge GAUTHRONET
Consultant – Président du Directoire ARETE

Notre cabinet d'expertise technologique est un bon observatoire des efforts technologiques considérables que déploient les entreprises commerciales pour améliorer leur connaissance client et diversifier les canaux de distribution avec notamment les entrepôts de données, les centres d'appels téléphoniques et le web. Depuis plusieurs années les investissements se concentrent aussi sur la mise en œuvre de logiciels de Gestion de la Relation Client, la GRC ou encore le CRM (*Customer Relationship Management*). Nous observons cette tendance plus particulièrement dans le monde des services et des établissements financiers, secteurs traditionnels qui peu à peu adoptent le CRM par l'intégration de progiciels ou la reconfiguration de leurs outils commerciaux traditionnels. La technologie du CRM, en ce qu'elle amplifie la collecte des données et permet de personnaliser les relations que les entreprises entretiennent avec leurs clients, n'est pas neutre du point de vue du respect de la vie privée des personnes. Notre expérience nous amène à faire trois grandes séries de constats :

1. En matière de gestion de la connaissance client et de la relation commerciale, une technologie ne chasse pas l'autre ; elles s'additionnent.

Il est d'usage de considérer qu'il y a trois grandes époques dans le développement des technologies du marketing : le marketing de masse, le marketing de segmentation et le « one to one », pour faire simple.

Aujourd'hui, nous constatons qu'à ces époques correspondent des générations technologiques qui cohabitent très bien et qui même s'imbriquent les unes avec les autres :

- *Le marketing de masse, celui des études de marché grâce auxquelles on réussit à déterminer la réceptivité des différentes catégories de clientèle à un produit et à en déduire le* design *existe toujours, que l'on sache, et c'est ce que l'on appelle le marketing produit.*

- *Le marketing des socio-types continue plus que jamais à produire ce que Philippe LEMOINE appelle les « artefacts statistiques ». On continue à segmenter les fichiers pour déterminer des profils de risques, par exemple, ou encore des propensions à consommer ou tout simplement des cibles de campagnes de marketing direct. Ce qui a changé évidemment au cours des années récentes c'est la quantité d'informations accumulées sur les clients et sur leurs comportements d'une part et d'autre part l'arrivée sur le marché d'outils de gestion de base de données sophistiqués et leur modélisation dans des* datarmarts.

  Ainsi, les entreprises n'en poursuivent pas moins la mise en œuvre de traitements statistiques extrêmement poussés ; cette sophistication culmine dans les établissements bancaires avec le calcul des notes de risque individualisées, la cotation Mac Donough, qui résulte de l'application des accords internationaux dits de Bâle II dont l'objectif premier est de proposer un nouveau ratio de couverture des risques par les fonds propres. Ces traitements manipulent mensuellement et suivant les modèles de calcul appliqués entre 200 et 300 informations par client.

- *Enfin, il y a le marketing* one to one *qui a été pensé il y a un peu moins de 10 ans et qui aujourd'hui devient une réalité dans un nombre croissant d'entreprises à travers notamment la mise en œuvre de logiciels de CRM.*

2. La logique d'utilisation du CRM dans ces entreprises reste majoritairement animée par une volonté d'enrichissement et de rationalisation des processus existants et ceci n'est pas neutre du point de vue de la protection des données et de la vie privée.

Plus précisément, les principaux objectifs poursuivis à travers le CRM sont au nombre de trois :

- *La collecte et l'accumulation de données qualitatives sur le client. C'est là une des innovations du CRM qui s'impose finalement comme un outil assez rustique permettant de documenter à la volée chaque relation qu'un vendeur est susceptible d'avoir avec son client. Il s'agit de capter l'information utile : les projets de voyage, les opportunités d'investissement, une intention de résiliation d'un abonnement, une promesse de remboursement dans une procédure pré-contentieuse. Au plan pratique, la méthode consiste à saisir du texte libre dans*

des zones ad hoc ou à cocher des cases dans des zones pré-contraintes afin de qualifier la relation que l'on vient d'avoir.

- *Le partage de l'information au sein des organisations complexes qui sont devenues multicanal. Dès lors se pose la question de centraliser et d'historiser en un lieu unique du système d'information commercial les données client, de sorte que la relation puisse être reprise là où elle a été interrompue la fois précédente, et ce quel que soit le canal emprunté. C'est là un des fondamentaux du one to one. Le CRM, a priori, répond bien à cet objectif. Il corrige aussi l'un des effets négatifs de la mise en portefeuille des clients qui conduit à des phénomènes de trop forte appropriation par les gestionnaires.*

- *Enfin, troisième objectif du CRM, est celui de la gestion événementielle de la relation client. Jusqu'à présent, la gestion événementielle s'opérait à travers des traitements informatiques assez banals consistant à déclencher une relation client à une date anniversaire ou à une échéance de contrat par exemple. Le CRM permet quant à lui « d'agender des actions », pour reprendre la terminologie appropriée ; cela signifie qu'en fonction des données qui auront été collectées, le commercial va demander à ce qu'une action soit remontée dans sa corbeille de tâches à telle ou telle date. Nous observons que cette gestion événementielle, alimentée également par des traitements de masse, est très délicate à régler. Dans la pratique, le CRM n'a pas encore réussi à casser la fâcheuse habitude qu'ont les entreprises de solliciter toujours les mêmes 20% de leurs clients.*

3. Le respect du client et de sa vie privée est une dimension absente aujourd'hui de la plupart des systèmes de CRM.

Dans l'esprit du concepteur du marketing *one to one*, la collecte d'informations s'inscrit dans une relation d'échange équilibrée et consensuelle. Don PEPPER et Martha RODGERS insistent particulièrement sur cette exigence et Seth GODIN l'a décliné de façon extrêmement pertinente dans le contexte de commerce électronique, à travers le concept de « *permission marketing* » : en deux mots, plus grandit la confiance entre le consommateur et l'institution commerciale, plus il est engagé dans la relation directe, stimulé par des promesses finement adaptées, plus il est enclin à donner de plus en plus de permission, permission de collecter plus de données sur son style de vie, ses passe-temps, ses centres d'intérêt ; permission pour être sollicité sur de nouvelles catégories de produits ou de services, permission pour recevoir des points cadeau ou des miles gratuits, un abonnement temporaire, etc. Au fur et à mesure que se construisent ces échanges, l'individu anonyme devient contact, prospect, puis bon client et enfin client fidèle. C'est le stade idéal de la relation participante avec le client, que Seth GODIN appelle le stade intraveineux.

Nous sommes malheureusement encore assez loin de l'application des ces principes-clés dans les entreprises des secteurs traditionnels qui s'essayent au *one to one* et au CRM. Que constate-t-on ?

- *Tout d'abord, les applications du CRM restent modelées par le marketing de masse et les statistiques : il est frappant d'abord qu'y figurent en bonne place dans la partie supérieure d'une fiche CRM, les données calculées par le système d'informations commerciales : les notes, les scores et les segments. De sorte que*

la relation reste vue principalement à travers le prisme de marqueurs d'identification dont le client la plupart du temps ignore l'existence et qu'il découvre seulement lorsqu'ils sont à l'origine de décisions qui lui sont opposées. Il est ainsi symptomatique d'observer à ce sujet que les établissements bancaires se sont empressés de faire figurer la cotation risques Mac Donough sur la fiche électronique du client ; sans pour autant en préciser le mode d'emploi pour les commerciaux.

- *Nous constatons également que le client n'a aucune idée et encore moins un quelconque contrôle sur la façon dont sont synthétisés et reportés dans l'outil de CRM les éléments saillants qui ressortent de son interaction avec l'institution commerciale. Ce phénomène est particulièrement inquiétant et les audits que nous réalisons régulièrement sur ces enregistrements montrent :*
  - que les équipes commerciales manquent cruellement de discernement et de formation quant au caractère approprié de l'information qu'il convient de collecter ;
  - que les entreprises commerciales des secteurs traditionnels ont parfois tendance à s'inscrire plutôt dans une relation de défiance voire d'exclusion à l'égard de certains de leurs clients.
- *Troisième constat, le CRM vu comme un outil de partage et de circulation de l'information au sein d'une grande organisation change complètement le statut de la confiance intime qui peut exister entre un client et son commercial. En d'autres termes, peut-on être intime avec une entreprise comme on peut l'être avec par exemple un conseiller en gestion patrimoniale auquel le client peut être amené à révéler des projets financiers extrêmement confidentiels ?*

En conclusion, nous pensons que les entreprises commerciales des secteurs traditionnels vivent dans l'illusion de la relation personnalisée, alors que tous leurs efforts restent concentrés sur une logique d'individualisation de la connaissance client. Il s'agit de deux approches radicalement différentes. Autant la personnalisation est sécurisante du point de vue de la vie privée car l'individu conserve une certaine maîtrise dans la relation, autant le schéma de l'individualisation renvoie aux questions bien connues de la problématique informatique et libertés qui sont celles de la loyauté de la collecte, de la circulation de l'information et de la finalité des traitements.

L'action de la CNIL sur ce terrain est majeure ; on pense notamment à son action concernant la décision automatique et les scores à la lumière du nouvel article 25 de la loi modifiée qui introduit désormais le régime de l'autorisation préalable ; à sa recommandation précisément concernant l'utilisation du ratio Mac Donough qu'elle préconise de réserver à l'instruction d'un crédit et de ne pas faire figurer dans un outil de gestion commerciale ; on pense enfin à son action contre la collecte de données stigmatisantes dans les zones en texte libre qui valent régulièrement des avertissements aux entreprises qui se laissent aller à des dérapages.

Mais il s'agit d'actions ponctuelles qui ne règlent pas le problème de fond qui est que l'on doit complètement repenser la gestion de la relation commerciale dans les secteurs traditionnels et revenir aux fondamentaux du *one to one* et de la personnalisation qui sont la confiance et le consentement dans l'échange. Pour cela

nous pensons qu'il faut creuser et promouvoir quelques grands cas d'expériences réussies dans la nouvelle économie, par exemple, et qui montrent comment on peut conjuguer la performance économique et le respect du client et de sa vie privée.

3. Confort : les traces de l'usage quotidien des réseaux

M. Marc FOSSIER
Directeur éxécutif en charge des technologies – France Télécom

M. Daniel KAPLAN
Délégué général de la Fondation Internet Nouvelle Génération FING

M. Marc FOSSIER

Directeur éxécutif en charge des technologies France Télécom

Plutôt que de rentrer dans le détail d'un certain nombre de problématiques techniques ou juridiques qui se posent à l'heure actuelle, je vais essayer de présenter la vision que nous avons de ce monde extraordinairement mouvant des communications électroniques au sens le plus large.

Il est d'abord intéressant de faire un retour sur les positions passées de France Télécom : Notre entreprise, au terme d'évolutions techniques très importantes s'est toujours considérée comme un opérateur de réseaux de télécommunication et non comme un fournisseur de services : il s'agissait de vendre un seul service, le téléphone, et toute notre intelligence technologique était focalisée sur ce domaine, dans l'amélioration des techniques de ce secteur : les réseaux, les fibres optiques, …

La situation a énormément changé depuis quinze à vingt ans, et ce, d'abord du fait de l'apparition du téléphone mobile. Au début, tout le monde a considéré qu'il s'agissait d'un système « en mobilité », mais il s'est rapidement transformé en un système de communication personnel. Ceci au point qu'aujourd'hui, entre 30 et 40% des appels téléphoniques mobiles sont passés de chez soi, bien que la téléphonie mobile soit en général plus chère et de qualité inférieure à la téléphonie fixe.

Tout ceci renvoie à un usage personnel du mobile, que ce soit grâce à son numéro, qui est un identifiant fort et totalement personnel, ou grâce à un certain nombre de facilités d'usage, qu'il s'agisse du carnet d'adresse ou de l'habitude d'emporter son terminal toujours avec soi, qui devient un objet « affectif ».

La deuxième grande évolution est l'arrivée de l'Internet, qui est par ailleurs un concept très évolutif et qui reste encore à préciser. Les premières applications grand public développées (navigation sur le Web avec le protocole http ou le courrier électronique) qui ont introduit des **dimensions proprement révolutionnaires dans l'organisation des communications personnelles**. En effet, ces technologies ont introduit une dimension « asynchrone », c'est à dire la possibilité de communiquer en temps différé, ce qui n'existait que très rarement avant, ou seulement sous forme

d'échec (le message sur le répondeur). Cela a des conséquences pour les grands organismes ou les grandes entreprises pour lesquels les seuls moyens de communication se résumaient à la voix, au coup de téléphone, ou à la note qui mettait en général entre une demi journée et plusieurs jours pour arriver à son destinataire. Ceci a complètement changé aujourd'hui avec la messagerie électronique.

La seconde innovation introduite par Internet est le multimédia, extraordinaire vecteur de nouveaux usages (transmissions d'images et de photographies par le net, de fichiers divers…).

Il faut aussi mentionner un point jusque là implicite dans les analyses sociologiques et qui depuis s'est incarné dans les nouvelles technologies : il s'agit du lien très fort entre contenu, de quelque nature que ce soit, et communication interpersonnelle. Il était jusque là connu des sociologues que les gens s'échangeaient plus d'informations à l'occasion d'un événement, comme un match de football, mais les outils Internet ont permis de matérialiser beaucoup plus ce couplage, que ce soit par des liens hypertextes permettant de rebondir d'une page web vers un forum, ou sur un courrier électronique, ou de transmettre par un simple lien cliquable facilement les coordonnées de tel site Internet.

Ces points sont très importants et ont permis de faire apparaître un certain nombre d'évolutions complètement nouvelles. Peut-être jusque là étions nous régis comme par notre seul hémisphère gauche en matière de communication, avec une démarche logique : « j'ai un message à transmettre à quelqu'un, donc je compose son numéro ». Aujourd'hui, regardez dans certaines tranches de la population, je pense notamment aux adolescents, fréquents utilisateurs des messageries instantanées, on est dans un système un peu différent : je me connecte, je vois qui est en ligne, et j'adapte mon message ou ma façon de communiquer à ceux qui sont en ligne (présents dans ma « buddy list »).

Voici ce que l'on a constaté jusqu'à présent dans l'usage de ces nouvelles technologies. Alors, on peut s'interroger sur ce qui va se passer à l'avenir ? Ces évolutions vont-elles se stabiliser ? ou au contraire ces technologies vont encore s'enrichir et se diversifier ?

Permettez à l'ingénieur que je suis de vous donner un aperçu de quelques grandes évolutions qui vont être au cœur des évolutions des technologies de l'information et de la communication pour ces prochaines années.

D'abord, il paraît évident pour tous les spécialistes, que le fameux protocole qui sous tend Internet (l'« Internet Protocol », l'IP), va devenir la base de toutes les télécommunications et de tous les échanges. Si ce problème peut paraître technique, il faut bien comprendre les conséquence que cela risque d'avoir. D'abord, « l'Internet Protocol » permet d'adresser n'importe quel contenu, à n'importe qui sur un même réseau. Ce qui est une révolution par rapport à ce que nous connaissions jusqu'à présent, où l'on distinguait un réseau « télex », un réseau téléphonique, des

satellites pour la télévision, des réseaux hertziens… Toutes ces technologies étaient cloisonnées et porteuses d'un service distinct.

Le protocole IP a beaucoup de défauts, il est moins efficace que d'autres protocoles plus spécialisés, car moins optimisé, mais c'est un protocole qui a **deux immenses qualités**. La première est qu'il **est utilisé par tous les acteurs**. Les développements, la recherche et les prix de revient en deviennent extraordinairement bon marché. Deuxième qualité de ce protocole : **il se sophistique, se raffine**, quitte à intégrer des éléments qui ne faisaient pas partie de la logique initiale. Á titre d'exemple, les « cookies » (qui n'ont pas été inventés pour créer des problèmes avec le respect de la vie privée), ont été inventés car le protocole qui permettait de naviguer sur le Web était insuffisant robuste pour gérer des sessions de communication, c'est à dire pour enchaîner des demandes successives.
Ainsi, lorsque vous passez d'une page Web à une deuxième page, il faut d'une manière ou d'une autre indiquer que c'est la même personne qui demande la deuxième page, donc il fallait faire un lien. Les cookies, qui paraissent intrusifs, ont donc été créés pour palier aux insuffisances d'un protocole qui initialement a été conçu pour permettre d'accéder à la documentation en ligne pour les chercheurs du CERN.

Ce petit exemple vous montre bien que ce protocole, assez rustique, assez pauvre, a été raffiné au fur et à mesure, jusqu'à devenir un support omniprésent.

Le second point, mais encore peu observé, est que le protocole IP, qui permet de transmettre n'importe quel contenu, de manière universelle, à tout le monde, peut aussi permettre l'émergence **de services totalement intégrés**. Il s'agit encore pour le moment d'un rêve, dans la mesure où nous restons dans des mondes relativement cloisonnés. L'idée par exemple d'enchaîner des communications de un à plusieurs, de plusieurs vers un, en **mélangeant du temps réel, du temps différé**… est quelque chose qui est technologiquement possible, mais les usages n'ont pas encore permis d'exploiter ces possibilités.

La seconde évolution technologique très importante concernant l'Internet, dont on commence à percevoir les conséquences sur les réseaux fixes, que ce soit en ADSL ou bientôt en fibre optique, **c'est le haut débit**.

Ainsi par exemple, le protocole IP ne permet pas encore aujourd'hui de faire efficacement de la communication par la voix sur des terminaux mobiles rattachés à des réseaux existants. Actuellement, ma voix est codée de manière bien plus efficace sur un réseau GSM. Sur des réseaux fixes, la situation est différente, le protocole IP permet des communications vocales très efficaces, en se greffant sur des réseaux vieux de cinquante ans. Mais sur le mobile, qui est une technologie datant des années 80, on code de façon plus efficace la voix en GSM que sur IP.

Par contre, dès que les réseaux mobiles auront des bandes passantes plus élevées, ce que l'on commence à voir avec l'UMTS, ou grâce au « WI FI » (réseau à plus courte portée), la voix sur mobile via le protocole IP sera une véritable alternative, permettant aussi d'ajouter la technologie de la visiophonie de façon simple.

Le haut débit, permet d'exploiter le plein potentiel de l'IP. Il va permettre dans un avenir proche de faire des assemblages de services. Mais déjà aujourd'hui des applications de ce type existent : un même protocole permet de faire de la téléphonie, de la télévision et permet un accès à d'autres services internet.

La troisième grande évolution technologique tient aux progrès extraordinaires de la radio. Des choses éblouissantes se font aujourd'hui en matière de transmission radio, qui ne manqueront pas de s'amplifier à l'avenir. **Grâce à de nouvelles fréquences, jusque là utilisées seulement par des applications professionnelles notamment militaires, on atteint des débits extraordinaires, avec une grande simplicité d'usage**. On peut aujourd'hui capter des satellites sous les toits, ce qui était impossible naguère. On peut transmettre des débits importants, sans la médiation des tours de radiodiffusion. Il est possible d'imaginer que bientôt, des techniques « d'ubiquité » vont se mettre en place permettant d'être en permanence connecté par une connexion radio, où que l'on soit.

Cela modifie les pratiques habituelles, d'abonnement à des réseaux cellulaires d'extérieur, mais l'on peut imaginer des continuités, notamment avec les téléphones fixes sans fil à la maison.

Quatrième grande évolution, qui fonctionne toujours par rupture, c'est l'impact de la micro-électronique dans les terminaux. Ceux-ci deviennent de plus en plus intelligents, ainsi aujourd'hui, les ordinateurs portables sont plus puissants que les PC d'il y a quelques années.

Les progrès des terminaux se traduisent par des ruptures d'usage périodiques : il devient soudain possible d'utiliser son PC pour de nouvelles applications, impossibles jusque là.

Par exemple, les protocoles de communication de « pair à pair » ou « peer to peer », utilisent et ne reposent que sur l'intelligence des terminaux. Ils sont d'ailleurs extrêmement instructifs pour les visions classiques des télécoms. Naguère, il existait des terminaux fonctionnant de façon assez simple (un téléphone, c'est un micro à grenaille, une pile, un fil, un transformateur et un interrupteur) qui reposaient sur le réseau pour établir des appels. La téléphonie de « peer to peer », c'est quelque chose qui n'utilise plus les compétences du réseau pour un appel. Lorsque vous voulez joindre votre correspondant, les différents logiciels implantés sur les différents correspondants possédant ce même logiciel, s'identifient les uns les autres, et tiennent à jour leur localisation et leur disponibilité sur le réseau.

Ce sont les terminaux entre eux qui effectuent la communication, s'appuyant simplement sur des fonctions de routage extrêmement simples du réseau et non plus sur des fonctions d'établissement de la communication. Pour le dire clairement, lorsque vous utilisez ce genre de logiciel, le réseau devient un simple transporteur, il ne fait que transmettre telle requête à un ordinateur, et n'assume plus son ancienne mission : établir une conversation électronique vers telle personne.

Ces nouvelles pratiques posent une question redoutable : Qui gère finalement cette intelligence d'adressage ?

Avant, l'UIT (Union Internationale des Télécommunications) gérait des plans de numérotage publics, et était encadré par un traité international. Aujourd'hui, on observe des fonctionnements communautaires à savoir que les acteurs disposant des mêmes logiciels et services, s'identifient les uns les autres.

Une bonne partie des usages se concentrent au sein d'un groupe fermé (amis, famille…), mais ils coexistent avec des technologies plus anciennes préservant toujours la possibilité de sortir de ces réseaux fermés et d'accéder à des correspondant qui eux sont universellement joignables car ils sont sur les plans d'adressage téléphonique historiques, et donc ouverts.

Lorsque vous joignez la troisième et la quatrième évolution dont je vous ai parlé, **soit les possibilités de la radio et l'intelligence des terminaux, vous obtenez** des choses dont on commence à voir les usages, qui sont ces fameuses **« intelligences d'ambiance** » ou « **poussières d'intelligence** », c'est à dire des objets extrêmement petits, dont le seul problème à l'heure actuelle n'est pas la miniaturisation mais l'alimentation en énergie, et qui peuvent être installés à peu près n'importe où.

Chacun de ces petits objets émet sur des courtes distances des ondes radio, identifie des congénères, et de proche en proche se maillent les uns par rapport aux autres et transmettent des signaux qui peuvent être des capteurs.

Les applications futures de ces « poussières intelligentes » laissent rêveur. Il est possible d'imaginer des utilisations militaires, mais même en restant dans le domaine des utilisations civiles, il est possible d'imaginer l'application de ces techniques pour la surveillance d'une installation domestique ou industrielle, (il s'agira alors de localiser un certain nombre de ces capteurs sur des endroits sensibles).

Le réseau en question sera alors un « réseau maillé », décentralisé, sans intelligence centrale. Ce sera la configuration automatique et intelligente de ces différents petits objets les uns par rapport aux autres qui fait le réseau dans son ensemble.

Ces nouvelles technologies semblent séduisantes sur le plan technologique, mais elles posent quelques questions importantes, renvoyant à certaines idéologies décentralisées. Des questions intéressantes y compris pour des usages industriels ou commerciaux : Qui est responsable de l'objet ainsi constitué ? Le responsable au sens juridique, au sens commercial. Á qui dois-je payer cette technologie ?

Si l'on compare le monde des transports et le monde de la communication, il apparaît que dans le monde des télécoms, nous sommes en train de passer d'un monde où il n'y avait que le train (c'est-à-dire une certaine qualité de service, garantie, et des ressources affectées), et un opérateur de voies ferrées, moyens plus coûteux, mais dont la qualité est garantie, et la responsabilité clairement identifiée, à une situation dans laquelle on est tous dans un modèle de routes : lorsque vous n'arrivez pas à destination à l'heure convenue, c'est la responsabilité de beaucoup d'acteurs : c'est

peut être votre véhicule qui est tombé en panne, ou c'est peut être l'infrastructure autoroutière qui est défaillante, ou encore la congestion due aux autres utilisateurs. **Ces modèles beaucoup plus diffus posent des problèmes de responsabilité**.

Lorsque vous avez un empilage de services et de prestations qui permettent d'offrir in fine le service bout en bout, il est toujours tentant lorsque l'on a une problématique de responsabilité, de recherche et de détection des infractions pénales par les services spécialisés de l'État, de se demander quel est le maillon qui, à défaut de la vision d'ensemble va me rendre compte de ce qui s'est passé, et, si l'on reprend les exemples précédents, rendre les infrastructures routières responsables des embouteillages.

Cette tâche nous revient souvent, car France Télécom et les autres FAI font partie des infrastructures les plus « basses », qui permettent de mettre en place ces logiciels de pair à pair. Il nous est éventuellement possible de savoir si tel utilisateur a mis en place un tel logiciel, notamment en observant les fluctuations sur la bande passante, mais quant à entrer dans les détails des communications réalisées, cela est non seulement pour le moment au delà de nos possibilités techniques, mais aussi au delà de nos possibilités contractuelles. Nous sommes en effet aujourd'hui simple fournisseur de certaines formes de connectivité, et non plus d'un service de bout en bout.

Ces révolutions technologiques sont assez structurantes, car elles bouleversent la chaîne de valeur. En effet, à partir du moment où tout est intégré, sur une infrastructure IP, **on arrive à ce paradoxe, qui secoue le monde des télécommunications : l'essentiel de notre chiffre d'affaire était jusque là la facturation** de la voix de bout en bout, alors que **sur des réseaux haut débit, la voix est très marginale**.
Par exemple, transmettre toutes les communications téléphoniques de la France, demande une fraction de plus en plus minime des réseaux de transport de données Internet. Aujourd'hui, la voix est un coût marginal d'un réseau plus vaste. On en voit la conséquence dans la tarification actuelle de la voix, qui ne cesse de baisser.

Est-ce que les clients veulent payer pour le transport ? Ce qui a été notre métier jusque là, le « transport » (une technologie servant à transporter d'un bout à l'autre une communication), et qui constituait le gros de notre chiffre d'affaire, tend à devenir de plus en plus marginal.

Actuellement, la demande du public va vers un certain nombre de fonctionnalités, qui, avec la baisse du coût du transport prennent une importance croissante. Il s'agit notamment de la « joignabilité », c'est-à-dire l'interconnexion des personnes quelque soient les réseaux traversés. Mais là encore des questions se posent : Comment le secteur s'organisera et qui sera la personne qui gèrera ce service ?

Deuxième sujet qui apparaît, qui était dans les usages, mais qui ne faisait pas partie du service en tant que tel, c'est ce que nous appelons **la gestion de « présence » ou la gestion de contexte** (que votre commission connaît bien sous le nom de la

« localisation »). C'est un sujet qui a été le centre de beaucoup de débats. Ce sont des procédures complexes à mettre en place, mais qui sont en voie de développement.

Le troisième point que je voudrais citer dans ces grandes tendances, c'est la **gestion des carnets d'adresse**, des listes de correspondants. Vous avez bien vu l'importance de cette notion dans tous les nouveaux protocoles de services qui sont apparus avec l'Internet, que ce soit la messagerie instantanée ou les communications de pair à pair. La gestion de ces carnets d'adresse est très importante. Elle correspond soit à la gestion de correspondants privilégiés sur un réseau ouvert, soit est au cœur d'une réseau de service. La messagerie instantanée repose sur la gestion de ce carnet d'adresses.

Un point qui devient important, qui est non seulement une des conséquences de la faiblesse du protocole IP mais qui est aussi une demande extrêmement forte de toutes les couches de la société, ce sont **les aspects d'identification et d'authentification**. On est très frappé sur le marché des entreprises de voir que l'objet de la facturation est moins le mégabit transporté, que la qualité d'intégration du système et la qualité des authentifications. **Il est très possible de travailler chez soi avec un PC et d'accéder au réseau interne de l'entreprise, mais cela n'est acceptable que si c'est sécurisé**.

Enfin, un sujet qui fera le lien avec l'exposé précédent, ce sont **les aspects de paiement**. Traditionnellement les télécommunications ont été un support voire un médias pour certaines transactions commerciales, et cela a été fait avec des outils en général assez captifs des différents supports utilisés : le kiosque audiotel, le kiosque minitel… **C'est un sujet qui est compliqué, car on est toujours dans des zones « grises » entre les fonctions des opérateurs de télécommunication et les fonctions bancaires**, au sens législatif du droit des moyens de paiement. Ce sont des sujets parfois **conflictuels**, même si les télécommunications sont des médiateurs souvent bien placés pour offrir des contenus, qui peuvent être soit des contenus éditoriaux, soit des prestations de service.

En conclusion, on est donc face à une situation extrêmement mouvante, assez paradoxale, qui se traduit à la fois par une séparation des différentes couches de services (avant un seul opérateur était responsable de la chaîne complète du service). Vous pouvez maintenant choisir l'accès chez l'un, l'identification chez un autre prestataire, avec une responsabilité partagée. Mais vous avez aussi une demande de personnalisation et une demande de responsabilité qui probablement emmènera à une situation très contrastée, avec des prestataires qui devront assumer leur responsabilité et des situations où les clients ou utilisateurs assembleront eux même leurs services.

Le problème des traces se pose avec d'autant plus d'acuité, elles ne peuvent être gérées par la responsabilité contractuelle ou législative de tel acteur, chacun ne pourra rendre compte que de la couche qu'il a lui même contribué à offrir. Cela amène à des débats compliqués, mais qui peuvent éventuellement trouver une analogie avec ce que l'on voit sur la route, où un certain nombre de règles ont été établies (nous considérons par exemple qu'il est nécessaires d'avoir un minimum de règles, en particulier sur les adressages, il est difficile de penser que des services

pourront naître sur des adressages complètement fermés qui confèrent des avantages aux premiers arrivés.

M. Daniel KAPLAN

Délégué général de la Fondation Internet Nouvelle Génération FING

Je voulais dire quelques mots sur la manière dont on peut évaluer à la fois l'évolution des usages et l'évolution des technologies, à la lumière des questions qui nous réunissent aujourd'hui, à savoir celles de l'identité et des données personnelles.

Je vais commencer par vous dévoiler un certain nombre de **résultats d'une enquête** que l'on a mené en ligne il y a un an de cela auprès d'internautes volontaires (donc ce n'est pas un sondage, mais un questionnaire permettant de dégager de grandes tendances et de tracer des portraits). Nous avions appelé ce questionnaire « vous et votre identité en ligne » et l'analyse de ce questionnaire a été réalisé par une étudiante en thèse de marketing. Cette étude sera présentée à l'université de Dauphine en juillet prochain.

Tout d'abord, lorsque l'on demande aux internautes si ils sont sensibles au thème de la protection des données transitant via Internet, ils répondent majoritairement oui. Lorsqu'on leur demande s'ils considèrent que lorsqu'ils agissent sur Internet, ils font face à des situations à risques concernant leurs données personnelles, ils répondent aussi par l'affirmative.

Il est donc intéressant d'observer les comportements construits par les internautes sont typiquement des comportements de gestion du risque. L'intérêt de ce questionnaire était de savoir quelles données ces internautes divulguaient, à qui, dans quelles circonstances, et en échange de quoi. La confiance est plus facilement accordée aux organismes publics, puis aux entreprises connues, avec lesquelles les internautes entretiennent déjà des relations.

Á qui donner ces informations : L'idée qui est ressortie est que l'on donne plus facilement des informations lorsque l'on achète un produit que pour autre chose. Ensuite, on va donner des informations pour obtenir des informations ou pour s'abonner à une newsletter. Au cours d'un jeu concours, on a des caractères assez divergents, on va avoir des personnes qui donnent les informations demandées et d'autres au contraire qui ne donnent rien. Il s'agit pour ce dernier point d'observer des divergences de comportement impliquant une vulnérabilité de la part de certaines catégories de la population.

La nature des données : la donnée la plus sensible pour les utilisateurs qui nous ont répondu, et de loin, c'est le numéro de téléphone portable (plus encore que le numéro de carte bancaire). Cela nous ramène sans doute à l'idée que le téléphone portable est devenu un outil extrêmement personnel, symbole de soi dans sa communication avec les autres. Le numéro de téléphone portable est devenu plus sensible que son numéro

de carte bancaire, et que le numéro de téléphone fixe. Des données moins sensibles, on y reviendra, sont l'âge, le sexe, et l'adresse de courrier électronique.

On est donc face à un comportement de gestion économique et stratégique du risque, ou l'utilisateur ne va pas répondre simplement « oui » ou « non », mais va s'inscrire dans une attitude de calcul.

On constate également que, dans la mesure où l'on se situe dans un domaine touchant à la protection de données personnelles et à la construction de soi, **tous ces internautes, actifs, ont plusieurs adresses e-mail et jonglent avec ces différentes adresses.** On a donc des formes de manifestations de son identité différentes, et huit sur dix personnes de cette population utilise des pseudonymes. Elles le font à la fois pour se protéger, pour ne pas être reconnues et pour d'autres choses, comme pour libérer la parole, pour être mieux compris en choisissant mon nom, pour gérer une forme de contexte par exemple.

Ce sont les comportements observables aujourd'hui, des comportements assez matures, mais liés malgré tout au fait que l'Internet aujourd'hui est un univers relativement pauvre. La vie est ailleurs. Toutefois, la situation semble s'inverser, on est de plus en plus souvent « en ligne », notamment grâce au téléphone mobile, s'il a les fonctionnalités correspondantes (GPRS).

Cette situation de connexion continue va s'étendre de plus en plus. Cela manifeste plus qu'une omniprésence des réseaux, cela manifeste une continuité des réseaux. Il y aura omniprésence des réseaux (ou que l'on soit, il y aura possibilité de se connecter aux réseaux, pour communiquer). Mais le plus important est que ces réseaux seront en continu. Il sera possible de se déplacer en restant connecté, en passant d'un réseau à l'autre. Aujourd'hui, plus que la question de l'omniprésence, la question de la continuité est importante. Et cette continuité pourra s'appliquer à une multitude d'objets, c'est-à-dire aux objets communicants traditionnels, mais aussi à toutes sortes d'objets qui seront en communication les uns avec les autres.

Quelles seront les implications futures de ces changements de comportements ? **La barrière à laquelle on avait fini par s'habituer entre le virtuel et le réel n'existe plus du tout aujourd'hui**. Le physique a une extension dans le numérique et inversement. Les capteurs, actionneurs qu'il y aura dans l'environnement ou que l'on portera sur soi seront des liens continus entre ces différents réseaux.

Tout cela n'émerge pas tant de ce que l'on pourrait qualifier de « folie totalitaire », mais d'une demande de services, de confort, ou de sécurité (par exemple la traçabilité alimentaire), de mobilité. Plus généralement il s'agit d'une demande née des contraintes de la vie moderne individualisée, dont les rythmes sont décalés, et pour autant dans laquelle nous avons au moins autant d'interrelations avec les autres qu'avant, mais sous des formes différentes.

Autre élément, ces moyens de communication ne seront pas que passifs. Cela signifie que nous serons nous même des capteurs, grâce à ces nouveaux moyens, nous pourrons surveiller notre monde et notre entourage. **Nous ne serons pas seulement**

les utilisateurs de ces services, mais aussi des « capteurs » et des « diffuseurs » de ces données omniprésentes et continues. On imagine bien entendu qu'à partir du moment où nos actes ont une existence numérique, cela multiplie les traces et les occasions de les produire, diffuser, stocker…

Ces traces « individuelles » vont à l'avenir probablement se combiner à la généralisation des traces permettant une identification et une authentification forte. Tout cela n'est pas neutre.

Ces techniques ne sont pas en elles même répréhensibles, je voudrais simplement m'attarder sur un seul point, à savoir **la tendance naturelle, dès lors que l'on dispose de ces techniques et qu'elles sont d'accès faciles (surtout si elles sont publiques), à s'en servir pour tout**.

L'occasion est trop belle : un système, éventuellement est agréé par l'État qui pousse à s'en servir, quelques fois à tort et à travers. Á ce niveau, si l'on ajoute à cela la dimension précédente, on est probablement dans une forme de risque, que je vais simplement illustrer en proposant à vous tous d'essayer de réfléchir aux nombre de transactions importantes que vous avez signé dans votre vie. Quelle est la proportion ? Probablement ultra-minoritaire. Ceci même dans vos relations d'affaires : est-ce que vous demandez toujours à vos clients, si c'est pour un service, de signer « avant » de commencer à faire quelque chose ? Si vous le faisiez, vous seriez sûr de perdre votre client.

Cela signifie que **ces technologies et techniques de la « confiance » ont émergé à partir de technologies de la défiance**. Au fond, la multiplication des technologies de la sécurité participe dans une certaine mesure du même mouvement que monsieur GAUTHRONET nous a décrit tout à l'heure, c'est à dire de l'expression d'une forme de défiance vis à vis du client. Les prestataires de services ou les agents commerciaux vont donc sécuriser leurs systèmes.

Lorsque l'on ajoute **toutes ces traces, nous sommes dans des dimensions troublantes au regard de ce qu'est la réalité d'une société dans laquelle la construction de soi est sans arrêt une forme de fuite vis à vis d'une origine biologique, familiale ou sociale univoque**. Dans ce domaine là, les régulateurs et les professionnels ont une responsabilité collective.

Sur la dimension de la régulation, qui reste absolument nécessaire, **il faut fixer des bornes**, il faut fixer ce qui est possible et ce qui ne l'est pas. Il faut bien voir que l'on est aujourd'hui en face de milliards de sources, installées par des gens différents. Je vous incite, si vous n'êtes pas allergiques à la science fiction, à lire un ouvrage qui a dix ans, qui s'appelle « l'âge de diamant », de STEPHENSON, et dans lequel il imagine un monde surveillé par des milliards de nano-caméra, accessibles au plus grand nombre. Dans ce cadre, un commerçant qui aurait envie d'aller espionner un concurrent enverrai sa nano-caméra, et vice versa. Á un moment donné, si vous vous promenez dans la rue et vous pouvez vous retrouver pris dans un nuage de nano-particules…

Cet exemple vous montre plus fondamentalement à quel point toutes ces données vont devenir difficiles à identifier. Il faut donc à la fois définir des règles, les faire respecter, et aussi **il va falloir explorer des formes autant décentralisées que possibles de liberté**. De ce point de vue là, on arrive assez rapidement à des formes de responsabilité des professionnels, y compris au regard de la « ligne du bas » (il y a un moment ou cette forme de défiance peut devenir mortifère en terme d'affaires).

Les professionnels vont devoir travailler pour le respect des droits informatique et libertés, mais ils vont aussi devoir se demander s'ils ont vraiment besoin de savoir telle chose sur leur client. Dans beaucoup de cas, ce n'est pas nécessaire. Le stockage des données pour le stockage des données est inutile, répandu, mais inutile. Il y a des milliers de données dont on sait pertinemment qu'elles ne seront jamais utilisées.

Une autre dimension, esquissée déjà, c'est ce que j'appelle la « **déconnexion action** ». Il s'agit de se dire que si la situation par défaut est celle de la communication, là où j'exerce ma liberté, donc là où il y a de la valeur, c'est dans la création de discontinuité. Le rôle de l'humain alors est de créer des discontinuités dans les systèmes techniques. Il faut avoir le choix de dire où non où je suis, de pouvoir éventuellement mentir sur sa géo-localité. Il s'agit de me laisser voir par mes amis à un moment, par mes collègues à un autre, de me laisser la possibilité d'être indisponible pour un certain nombre de gens, de me travestir, de travestir le contexte, etc…

Il y a un énorme travail de recherche et de scénarisation à mener sur ces points. Il faut que les gens puissent réellement exercer cette possibilité là, et il faut réfléchir sur quelles possibilités offrir aux utilisateurs, au fur et à mesure, dans la réalité du tissus quotidien.

Voilà un certain nombre de pistes de création de valeur et de création d'espaces de liberté, dans ce contexte technologique qui est assez différent et qui est en train de s'ouvrir à nous.

Parce que les **capacités de stockage**, de traitement et d'échange d'information **seront demain** répartis dans l'espace numérique et physique, **à un niveau sans commune mesure** avec celui que nous connaissons aujourd'hui, on a besoin de trouver des solutions de principe, de contrôle, mais également des **solutions les plus décentralisées possible**. Dans le cas contraire, nous serons dans la fiction d'une réalité d'une maîtrise de l'identité et de la circulation des données personnelles. Parce que tout ce que nous ferons aura une forme de continuité numérique, et c'est bien dans la création de cette discontinuité que réside notre liberté et l'exercice de notre volonté.

Pour terminer je voulais insister sur le fait que je suis persuadé que tous ces dispositifs devront être pensés par les professionnels, au moment de la création des artéfacts, je vous recommande à ce sujet un livre d'un designer nommé **Adam GREENFIELD**, appelé « Every where ». GREENFIELD s'est posé des questions proches de celles que je viens d'aborder, mais de son point de vue de designer, en se demandant si ce que nous créons avec l'intelligence ambiante, l'informatique en

continu, c'est à la fois un univers de services, qui répond à de vrais besoins, et un potentiel de débats sans commune mesure puisque l'on ne joue plus seulement avec des symboles et des informations, mais avec des corps, de l'espace. Donc si l'on veut résumer : trois millions de virus dans des ordinateurs c'est très ennuyeux, trois cent virus dans les pacemakers, c'est dramatique.

GREENFIELD dit qu'il va falloir réfléchir à la nature des systèmes d'intelligence ambiante, et il propose **cinq principes, à discuter et à débattre**, qui paraissent intéressant à réfléchir, à la fois **par des concepteurs de service, par des juristes et par des politiques**.
Le premier est celui de **l'innocuité par défaut**. Le système doit être configuré par défaut de manière à ne pas pouvoir mettre en danger la sécurité physique, matérielle ou biologique de son utilisateur.

Le second principe, c'est celui de **la transparence** : qu'est-ce que je fais, pour quelle finalité ? qui est responsable ?

Le troisième principe est celui de **la considération** : ne pas faire perdre la face à son utilisateur.

Le quatrième est **l'économie de temps ou la simplicité** : ne pas compliquer indûment les tâches quotidiennes. C'est à dire ne pas imposer la logique de système à des utilisateurs.

Le cinquième principe consiste à d'**admettre le refus**, à considérer que c'est une situation normale de pouvoir refuser une technologie et préférer « passer en mode manuel ». Cela est très difficile, car une part importante de l'économie des systèmes, consiste à supprimer le mode de fonctionnement classique. Arriver à imaginer comment on va permettre au contraire à l'autre mode de fonctionnement de continuer à exister tout en recherchant les gains de productivité en terme de service, est difficile, mais c'est selon moi des choses que l'on a besoin de regarder ensemble.

MARDI 8 NOVEMBRE 2005

A. LA LOI INFORMATIQUE ET LIBERTÉS (1978-2004) EN QUESTIONS

Présidence Mme. Martine LOMBARD 9H00-12H30

Mme Martine LOMBARD
Professeur à l'université de Paris II (Panthéon-Assas),
Directeur du centre de recherche en droit administratif (CRDA)

Le thème qui va nous occuper ce matin est le suivant : « *La loi informatique et libertés en questions* ». Il est symptomatique de l' « intranquilité » de ce secteur, intranquilité nécessaire, sinon vitale, car si nous sommes entrés comme le disait le président de la CNIL, Alex Türk hier, dans l'ère de « big brother », trop d'ordre et trop de quiétude seraient beaucoup plus inquiétants que cette intranquilité.

Pour le juriste de droit public que je suis, la Commission nationale informatique et libertés a toujours été une sorte de guetteur atypique qui jette le trouble, y compris dans l'ordre trop bien huilé des institutions administratives et du droit de façon plus générale. Heureusement, chacun a oublié la perplexité éprouvée il y a vingt cinq ans, lorsque avait été créée cette première Autorité Administrative Indépendante, que plusieurs juristes considéraient comme un « *OVNI* », ou un objet juridique non identifié, mais qui depuis a largement fait école. Mais la CNIL surtout nous a habitué à la force paradoxale de ce que nos amis anglo-saxons appellent la « soft law », qu'il ne faut pas comprendre comme un droit formellement dur mais bavard et inutile, ce qui n'est pas le registre d'action de la CNIL, je parle plutôt d'un droit dont les formes sont « molles » en apparence, un droit fait d'avis, de recommandations, de communiqués, d'enquêtes… Mais un droit qui pourtant parle fort, qui est efficace, et cela à force de persuasion et de conviction. Pour que ce droit soit efficace, encore faut-il qu'il soit soumis à une remise en question permanente. Et c'est bien l'intérêt des débats de ce matin, qui doivent contribuer à cette constante remise en question.

Après un exposé introductif sous forme de question : « ***Le cadre juridique est-il adapté aux enjeux contemporains ?*** », nous aurons trois ensembles de réponse, **la réponse du politique, la réponse de l'ordre public et la réponse de l'industrie**, des réponses dont je ne doute pas qu'elles suscitent à leur tour des questions. Les questions viendront aussi de vous et je veillerai à ce que vous puissiez les poser, après chaque groupe d'intervention.

Sans attendre, je voudrais donner la parole au professeur Jérôme Huet, qu'il n'est pas nécessaire de présenter ici, tant il est bien connu par ses travaux éminents en la matière, qu'il s'agisse de ses ouvrages sur le droit de l'informatique, sur le code de la communication, ou de ses articles sur les contrats électroniques, sur le commerce électronique, et d'une façon plus générale, sur le droit de la communication. Par ailleurs, comme professeur à l'université Paris II, mon collègue Jérôme Huet dirige un master recherche au sein de cette université, ainsi qu'un master professionnel, tous les deux tournés vers le droit de l'informatique et du multimédia.

1. Exposé introductif : Le cadre juridique est-il adapté aux enjeux contemporains ?

M. Jérôme HUET
Professeur à l'Université de Paris II (Panthéon-Assas),
Directeur du Centre d'études juridiques et économiques du multimédia (CEJEM)

Le thème de la matinée est intitulé « *La loi informatique et liberté en questions* », ce qui est déjà un défi, car il faut trouver quelles sont les bonnes questions. Et, plus précisément, il m'est demandé de déterminer si « *le cadre juridique est adapté aux enjeux contemporains* ».

Le sujet est vaste car le « *cadre juridique* » dont il s'agit déborde de beaucoup la loi elle-même : il englobe l'ensemble des normes existant en la matière, notamment la directive communautaire de 1995 transposée dans notre droit en 2004, et le décret d'application de la loi de 2004, adopté en 2005, sans compter divers autres textes sur lesquels on reviendra.

Ce « *cadre juridique* » est-il adapté à la société d'aujourd'hui ? En répondant à cette question, on risque de faire des mécontents, car il n'est pas sûr que ce cadre convienne à tout le monde. Il est donc nécessaire de se demander à qui, et sans doute aussi à quoi, ce droit des données personnelles peut-il, ou doit-il, être adapté.

1. Le cadre juridique de la protection des données à caractère personnel

Avant tout, commençons par rappeler quel est exactement le « *cadre juridique* ». La loi du 6 août 2004, venue transposer la directive adoptée en la matière par la Communauté européenne en 1995, est un texte qui a été longuement mûri. C'est une loi complexe qui apporte des modifications significatives au droit mis en place par la loi de 1978, qu'elle modifie de fond en comble ; elle est désormais assortie d'un décret d'application du 20 octobre 2005.

Il y a là un bouleversement dans le système de protection juridique des données personnelles, ne serait-ce qu'en raison de la portée que la loi de 2004 donne au régime d'autorisation préalable des traitements, qui s'applique désormais aux entreprises privées. Le décret d'application de 2005, lui-même, contient des dispositions très importantes et, notamment, il aménage l'institution du « *correspondant à la protection des données* ». Ces modifications vont nécessiter des efforts d'adaptation de la part des destinataires des règles en cause.

Le renouvellement du droit est considérable. Dans la loi de 1978, il y avait 48 articles, si l'on compte les sanctions pénales qui ont été intégrées par la suite dans le nouveau code pénal. Aujourd'hui, la loi modifiée par celle de 2004 en compte 72 : à

peu près le double, étant entendu que les dispositions pénales ne sont pas intégrées dans cette loi ; qui plus est, les articles sont beaucoup plus longs. L'ensemble est nettement plus conséquent que celui dont nous disposions en 1978.

On peut dire que la loi de 2004 est un texte de qualité. J'ai été très inquiet quand j'ai vu les premiers projets circuler, mais petit à petit, le travail législatif a porté ses fruits. Le texte comporte des nouveautés, en particulier le mécanisme du « *correspondant à la protection des données* ». Il comporte aussi des clarifications : ainsi, le régime d'autorisation dont la directive prévoit qu'il s'impose pour les traitements présentant un certain degré de dangerosité va jouer pour les traitements figurant sur la liste établie par l'article 25 de la loi. Il y a là une transposition à la française.

La directive européenne remonte à 1995 et, de ce fait, presqu'une dizaine d'année s'est écoulée avant sa transposition en France. Le texte européen constitue une vraie directive, car il laisse une marge de manœuvre significative aux Etats membres pour élaborer leur propre droit en la matière. Pour la France, la liberté ainsi reconnue était appréciable car la loi de 1978 avait produit ses effets depuis un certain temps, des habitudes avaient été prises, des solutions retenues et des décisions rendues.

Pour donner une idée plus complète du cadre juridique, il faut signaler aussi l'existence d'une directive de 2002 sur la protection des données personnelles dans les communications électroniques, qui remplace une directive de 1997 concernant secteur des télécommunications. Directive qui avait été déjà transposée, pour partie, dans la loi de 2001 sur la sécurité quotidienne. Il s'y ajoute quelques dispositions de la loi sur la confiance dans l'économie numérique du 21 juin 2004, la « LCEN », notamment celles concernant le « spamming ». La directive de 2002 et la LCEN traitent de la sollicitation par voie de courrier électronique et elles ont retenu, pour lutter contre ce fléau, la solution la plus favorable aux internautes, celle dite de « l'opt-in », c'est-à-dire de l'autorisation préalable de la personne concernée. Mais on sait que cette solution n'a pas encore permis d'éradiquer le phénomène.

Le cadre juridique a donc été rénové et étoffé, et il offre de multiples potentialités. Mais est-il adapté pour autant. Nous nous demanderons d'abord « *à qui il est adapté* ? », puis nous tenterons de déterminer « *à quoi est-il adapté* ? »

2. À qui est adapté le cadre juridique de la protection des données à caractère personnel ?

On ne peut pas faire le tour de tous les acteurs concernés. J'évoquerai deux catégories de personnes, qui me paraissent être les plus importantes : les individus et les entreprises.

2.1. Le cadre juridique est-il adapté aux individus ?

La loi sur les données personnelles protège les individus, les personnes physiques et non les personnes morales. Les individus sont ceux qu'on appelle volontiers les « *personnes concernées* » par les traitements. Est ce que la loi leur est adaptée ?

La loi de 2004 comporte des avancées significatives en leur faveur. D'abord la connaissance de la loi s'est améliorée. Elle est rendue plus facile d'accès car le texte est plus clair, en particulier dans le détail des prérogatives qu'il reconnaît aux personnes. Les droits sont mieux identifiés, ils sont diversifiés, ils ont une gradation : « *information préalable* », « *droit d'opposition* », « *consentement* »…

De leur côté, les obligations des responsables des traitements sont, elles aussi, mieux définies et, souvent même, clarifiées. Cela permet aux personnes concernées de se piloter plus aisément dans cet univers difficile. Elles savent mieux à qui s'adresser du fait que la loi prévoit que chaque traitement doit avoir un « *responsable* ». Cette règle ne figurait pas dans la loi de 1978, ce qui était probablement un oubli de ses rédacteurs.

Les personnes concernées bénéficient aussi du fait que l'acquis de la loi de 1978 a été fermement maintenu : droit d'accès et de rectification des données personnelles, consécration sans ambiguïté de la notion de données sensibles, voire très sensibles... La notion a été étendue aux données de santé, ce que la CNIL avait d'ailleurs commencé à faire sous l'empire de la loi antérieure. Cela n'ira pas sans soulever des difficultés considérables d'interprétation, mais c'est aussi un progrès pour les personnes concernées. Autre consécration de l'acquis, encore : la durée limitée de la conservation des données, qui est un des traits essentiels du dispositif de la loi Informatique et Libertés.

La question de la durée de conservation a été au centre de la recommandation de la CNIL concernant « *l'alerte éthique* » dans les entreprises car l'un des outils dont s'est servi la CNIL pour cantonner les risques pouvant en résulter est la durée de conservation des dénonciations entre salariés. En effet, si l'information donnée sur un salarié s'avère inexacte, il est impératif qu'elle soit effacée sans délai. De fait, on pouvait craindre que des dénonciations injustifiées concernant des collègues de travail ne traînent indéfiniment dans des fichiers.

Par ailleurs, la maîtrise des personnes sur les données les concernant a été renforcée grâce à l'exigence du consentement préalable à figurer dans un fichier. Certes, ce consentement n'est pas toujours requis ; il existe des exceptions, assez nombreuses au demeurant ; néanmoins, le contrôle des individus sur les informations personnelles s'en trouve accru. Il en va de même en raison des dispositions consacrant l'information des personnes concernées, en cas de cession de fichiers, tout comme en cas de collecte de données auprès d'elles.

Mais, avant tout, l'amélioration de la protection des personnes va résulter de la portée nouvelle, radicalement plus large, donnée au régime d'autorisation pour des traitements du secteur privé. Le phénomène est tout à fait nouveau, car auparavant, dans le secteur privé, les traitements ne faisaient l'objet que d'une déclaration. Certes, on sait que, non sans audace, la CNIL a utilisé la rétention du « *récépissé* »

de déclaration – récépissé sans lequel le traitement ne pouvait pas être mis en œuvre – pour influer sur le contenu des traitements, pour faire modifier le contenu des déclarations, attitude qui a été condamnée par le Conseil d'Etat. Mais, en pratique, cela a permis à la CNIL d'exercer un certain contrôle sur les traitements soumis à simple déclaration.

Dorénavant, le régime d'autorisation va largement s'appliquer pour les traitements du secteur privé. La liste qui est donnée par l'article 25 de la loi est très compréhensive et certaines catégories de traitements visées peuvent être nombreuses : il en va ainsi des traitements ayant « susceptibles… d'exclure des personnes du bénéfice d'un droit *». Cela va concerner de nombreuses personnes qui entretiennent des relations avec les entreprises : que ce soient les salariés à l'intérieur, ou les clients à l'extérieur. Les traitements de données aujourd'hui servent souvent à cela. Cette disposition permet de comprendre pourquoi les dossiers concernant «* l'alerte éthique *» ont fait l'objet d'une procédure d'autorisation. Il y a donc là un progrès considérable pour les individus.*

Pour autant, des incertitudes subsistent dans le dispositif législatif, qui peuvent être nuisibles. S'agissant du consentement préalable, parmi les exceptions prévues à l'article 7 de la loi figure une hypothèse particulièrement vague : celle où « *l'intérêt légitime poursuivi par le responsable du traitement* » peut l'emporter sur « *les droits et libertés fondamentaux de la personne concernée* ». La formule est susceptible de justifier bien des dérogations à l'exigence du consentement préalable.

Certes, les rédacteurs de la loi de 2004 ne sont pas responsables de cette formule ambiguë : elle figure dans la directive. Elle n'en est pas moins dangereuse, plus encore dans la loi de 2004 que dans la directive européenne de 1995, car celle-ci ne comporte pas de sanctions pénales, contrairement à la loi de 2004.

Autre ambiguïté pour les personnes concernées : la notion même de « *consentement* ». L'exigence d'un consentement peut apparaître comme un progrès. Mais dans le même temps, elle est à double tranchant, car on ne sait pas exactement ce qu'est le consentement. Il est fait usage de cette notion de façon surabondante dans la loi, tout comme dans la directive. L'article 7 de la loi pose le principe général du consentement préalable, mais il y a des exigences spéciales de consentement, avec des formulations variées selon les textes. Pour les « *données sensibles* », la personne concernée peut consentir à leur traitement, mais en ce cas, il faut un consentement « *exprès* ». En ce qui concerne les données médicales, et plus précisément des prélèvements biologiques identifiants, l'article 228-18 du code pénal parle d'un consentement « *éclairé et exprès* ». Pour les transferts internationaux de données vers des pays ne répondant pas aux standards de la communauté européenne, là encore on exige un consentement « *exprès* ».

Or, sur bien des points le mystère est entier. Comment le consentement doit-il être donné ? Quelle doit être l'information de la personne concernée sur le traitement auquel elle consent ? Le consentement peut-il être rétracté *a posteriori* ? Il faudra donner des réponses à toutes ces questions.

Voilà des sujets sur lesquels les personnes concernées vont s'interroger, et si elles sont perplexes, elles hésiteront à faire valoir leurs droits.

2.2. Le cadre juridique est-il adapté aux entreprises ?

Le droit des données personnelles doit être également adapté aux organismes auxquelles il a vocation à s'appliquer, aux institutions, aux administrations, aux entreprises… Les administrations se sont pliées assez facilement exigences de la loi Informatique et Libertés, ne serait-ce que pour des raisons médiatiques.

Ce souci est moindre pour les personnes privées, lesquelles vont, sans doute, être tentées jouer en la matière « *au chat et à la souris* ». La relative faiblesse de moyens de la CNIL peut leur faire penser qu'elles risquent d'échapper aux sanctions. On sait qu'il n'y a pas eu beaucoup de sanctions pénales mises en œuvre depuis 1978. Certes, il y a maintenant des sanctions administratives qui vont permettre de renforcer la vigueur de la loi, mais en ce qui concerne les entreprises, il faut certainement compter avec la « *tolérabilité* » des règles juridiques.

Toutefois, on peut estimer que la loi leur est relativement bien adaptée. Des progrès ont été faits depuis 1978. Avec le développement considérable qu'a connu l'informatique, il était difficile de conserver un droit trop coercitif. Il y a donc eu des allègements dans la contrainte juridique, qui étaient très attendus, notamment dans le régime de la déclaration des traitements, en donc pour les traitements ne présentant pas de risques particuliers pour la vie privée et les libertés.

La porte est a été ouverte par la directive de 1995 et le législateur, en 2004, a exploité les possibilités ainsi offertes. Dans bien des cas, la déclaration est simplifiée, voire écartée ; elle peut même se faire par voie électronique. On a maintenu les déclarations simplifiées prévues par la loi en 1978 pour les traitements les plus classiques : il faudra, simplement, rajeunir certaines des normes adoptées par la CNIL pour ce type d'hypothèse. Mais surtout, dans les situations où le traitement peut être considéré comme banal, il n'y aura plus lieu à déclaration du tout.

Par ailleurs, la possibilité de recourir au « *correspondant à la protection des données* » constitue pour les entreprises un moyen de gérer de manière efficace et sûre les questions de traitement de données personnelles. Cette fonction, normalement assumée à l'intérieur de l'entreprise, peut être externalisée pour les petites ou moyennes entreprises : il sera possible pour elles de recourir à un prestataire extérieur. Cela permettra de standardiser ce type de fonction, de la professionnaliser.

Une autre simplification apportée par la loi de 2004 tient à la manière dont est clarifié le statut de l'entreprise sous-traitante à laquelle sont confiées des données personnelles (article 25 de la loi de 1978). Quant aux transferts internationaux de données, ils peuvent être effectués dans le cadre de clauses contractuelles, ce qui apporte de la souplesse et une sécurité juridique.

Tous ces éléments nouveaux constituent un progrès, une simplification pour les entreprises. C'est seulement lorsque les traitements présentent une certaine dangerosité pour les droits et libertés que les contraintes se renforcent.

Cependant, la loi de 1978, telle que modifiée en 2004, comporte aussi pour les entreprises une part de flou. On le constate notamment à propos des obligations incombant aux responsables des traitements (articles 32 et suivants de la loi de 1978), et tout particulièrement s'agissant de l'information à donner aux personnes concernées en cas de cession de fichiers. Les textes applicables reprennent pour l'essentiel les articles 10 et 11 de la directive, qui sont passablement difficiles à comprendre. Les exigences sont complexes, et sans doute excessives. On imagine la perplexité d'un chef d'entreprise à qui l'on dira que s'il recueille des données à caractère personnel auprès d'une personne, celle ci doit recevoir toute une série d'informations : identité du responsable du traitement, finalité poursuivie par ce dernier, caractère facultatif ou obligatoire des réponses…, sans compter qu'il faut indiquer aux intéressés les droits qu'ils détiennent en vertu « *des dispositions de la section 2 du présent chapitre* »… Or, ces droits sont détaillées dans plusieurs rubriques : droit d'opposition, droit d'interroger, droit de contester la logique, droit d'exiger la rectification…

Peut-on résumer ces différentes dispositions ou faut-il reprendre toutes ces informations ? Les sanctions pénales, qui sont prévues dans le décret de 2005, même si elles ne sont pas très lourdes, incitent à être le plus précis possible.

De plus, la question se pose de savoir comment l'entreprise pourra conserver la preuve de qu'elle a bien donné l'information requise. Elle devra aussi garder la trace du consentement préalable des intéressés lorsqu'il est exigé. Or il n'est pas facile de conserver une telle preuve : preuve écrite sur papier ? On mesure la lourdeur du procédé. Mais il est vraisemblable que certains opérateurs s'y plieront. Les mieux à même de collecter des données personnelles sont ceux qui peuvent faire signer un contrat aux personnes concernées (contrat de fidélité dans un magasin), ou peuvent leur faire remplir un questionnaire (gestionnaires de mégabases de données comportementales). Ces contrats ou ces questionnaires contiennent une clause précise selon laquelle les données recueillies peuvent être utilisées à différentes fins que le détenteur des données se réserve d'exploiter. En revanche, sur les réseaux numériques, le consentement sera donné sous forme électronique, et en conserver la preuve s'avèrera difficile.

Cette complexité va pousser certaines entreprises à faire de la résistance, notamment sur l'internet. Il en ira notamment ainsi en ce qui concerne les « *cookies* », car la loi précise, dans son article 32, que toute personne utilisatrice de réseaux de communication électronique « *doit être tenue informée de la finalité de toute action tendant à accéder par voie de transmission électronique, à des informations stockées dans son terminal de connexion* ».

S'agissant des personnes auxquelles il s'applique, on peut donc dire que le « *cadre juridique* » est assez largement adapté. Mais une seconde question se pose qui est de savoir à quoi la loi est adaptée ? Quels sont les enjeux contemporains ?

3. À quoi la loi est-elle adaptée ?

Parmi ces enjeux, j'en signalerai deux sortes, à titre d'illustration. La loi est-elle adaptée aux besoins de sécurité ? Enjeu contemporain s'il en est. Plus largement, on doit se demander si la loi est adaptée à la mondialisation ? Autre enjeu contemporain.

3.1. La loi est-elle adaptée aux besoins de sécurité ?

Sur ce point, la loi est encore incomplète. On peut même penser que l'essentiel se trouve en dehors de la loi. Des dispositions figurent dans la loi pour la confiance dans l'économie numérique, (article 6 II-1), où il est prévu que les fournisseurs d'accès et d'hébergement détiennent et conservent les données de nature à permettre l'identification de quiconque a contribué à la création de contenu. Dans le même temps, la loi relative à la sécurité quotidienne, du 15 novembre 2001, a introduit dans Code des postes et des communications électroniques un texte, devenu l'article L. 34-1, intéressant les opérateurs de télécommunications. Cet article vise aussi bien la téléphonie que l'internet, aussi bien la communication privée que la communication publique.

Les opérateurs de télécommunications, et donc les fournisseurs d'accès, se trouvent dans une situation extrêmement difficile. Le texte n'a pas changé depuis 2001 et les opérateurs se trouvent obligés de faire une chose et son contraire, en même temps ou presque. Il doivent, en principe, effacer ou rendre anonymes toutes les données relatives à une communication dès qu'elle est achevée : c'est la confidentialité. Dans le même temps, ces opérateurs doivent être vigilants, car ils doivent aussi, pour les besoins de constatation ou de poursuite d'infractions pénales, différer l'effacement ou l'anonymisation des fichiers et conserver les données de connexion pendant une année…

Cette disposition a fait dire, à la suite des événements tragiques de 2001, que la France faisait partie des pays « *liberticides* », à côté d'autre pays qui comme les Etats-Unis, mettaient en place le « *Patriot Act* ».

La Communauté européenne devrait prévoir un standard européen de conservation des données de connexion, que ce soit pour la téléphonie ou pour les communications électroniques, et l'on hésite entre un an et deux. Voilà un point sur lequel le droit n'est pas encore totalement clarifié. En tout cas, il faudra que le dispositif retenu ne porte pas sur le contenu des communications, mais uniquement sur les données de connexion elles-mêmes, qui certes ont un caractère indiscret, mais qui menacent moins les libertés.

Plus largement, et par-delà ce qui concerne la conservation des données de connexion, c'est l'identification même des personnes qui mettent du contenu à la

disposition du public sur l'internet qui sera la clé du bon fonctionnement de la communication en ligne dans l'avenir. Or, cette question est loin d'être simple, et loin d'être résolue.

3.2. La loi est-elle adaptée à la mondialisation ?

Il faut tenir compte aussi du fait que les données circulent par-delà les frontières. C'est un point sur lequel il n'y avait rien dans la loi de 1978. Il était simplement dit que, dans la demande d'avis pour une administration, dans la déclaration soumise par une personne privée, l'on devait indiquer s'il pouvait y avoir un transfert international des données personnelles.

Aujourd'hui, on prend la chose beaucoup plus au sérieux. Dès 1995, la directive avait prévu dans deux articles, les articles 25 et 26, qu'à l'intérieur de l'Europe, la circulation des données personnelles est libre, car l'ensemble des Etats membres connaissent un niveau de protection d'un niveau élevé, mais qu'il est interdit de faire circuler les données à caractère personnel en direction de pays tiers à la communauté qui ne présenterait pas un niveau de protection adéquat. Le terme « *adéquat* » n'est pas facile à interpréter, pas plus que celui que le législateur français a choisi : il faut que le degré de protection soit « *suffisant* ». On sait maintenant quels sont les pays présentant un niveau de protection adéquat pour la protection des données personnelles. Il n'y en a pas beaucoup : la Suisse, le Canada et l'Argentine.

A destination des autres pays, il serait interdit d'effectuer un transfert international de données. La question s'est posée dans les rapports avec les Etats-Unis et il a fallu trouver une solution : la Commission européenne a négocié avec les Etats-Unis un accord, dit « l'accord de sphère de sécurité » (en anglais les principes du « safe harbour »). Cet accord prévoit un mécanisme ingénieux. Les américains n'ont pas voulu se soumettre à un régime contraignant : ils ont souhaité panacher la rigueur et le volontariat. Dans l'accord passé, le niveau de protection n'est pas aussi élevé qu'on pouvait le souhaiter. Le principe de protection n'est pas celui du consentement préalable, mais des mesures sont prévues : l'information des personnes concernées, le droit de rectification, la durée de conservation des données… Et le mécanisme retenu est que les entreprises américaines ont la possibilité d'adhérer à ce régime de protection pour pouvoir échanger des données personnelles avec les entreprises européennes. C'est ingénieux, ce n'est pas suffisant, mais ce n'est pas si mal.

Pour les autres pays, on a mis au point un mécanisme, jadis préconisé par le Conseil de l'Europe : un modèle de clauses contractuelles pour l'échange international de données personnelles. Ce mécanisme, lui aussi, est insuffisant, mais il vaut mieux que rien. L'idée est d'encadrer des échanges de données personnelles entre des entreprises, entre des entités de pays européens et de pays ne présentant pas un niveau de protection adéquat. Dans ces clauses, les entreprises s'engagent à transmettre et conserver les données dans des conditions offrant une certaine sécurité. Et les personnes concernées se voient reconnaître le droit de rechercher la responsabilité des entreprises en cause en cas de violation de leurs obligations.

On le constate, ces solutions apportent des réponses, certes minimalistes, mais des réponses concrètes, à la question de la circulation internationale des données personnelles.

Pour ce qui est, enfin, des données personnelles mises à disposition du public sur un site internet, le droit actuel est radicalement inadapté. On le constate dans une décision rendue par la Cour de justice des Communautés européennes, dans un arrêt « *Lindqvist* », du 6 novembre 2003 : il s'agissait d'un site sur lequel figuraient des données concernant des personnes travaillant à titre bénévole, en Suède, dans une église protestante. L'exploitant du site avait fait l'objet de poursuites pénales pour n'avoir pas respecté la loi suédoise sur la protection des données. Le tribunal s'est demandé si, de surcroît, il n'y avait pas également un transfert international de données et, sur ce point, a saisi la CJCE. Celle-ci a considéré, de manière fort pragmatique, qu'il n'y a pas là un transfert international de données. De fait, celui qui met en ligne ces données n'a pas voulu procéder à un transfert international de données personnelles. Pour autant, il est difficile de nier que, mises ainsi à la disposition de n'importe qui dans le monde, les données en cause peuvent circuler par-delà les frontières, et atteindre des pays ne présentant pas un niveau de protection adéquat…

Le droit des données personnelles, rajeuni au niveau européen par la directive de 1995, modernisé en France par la loi de 2004, s'avère ainsi plus protecteur des personnes concernées et, sans doute aussi, mieux adapté aux entreprises qui peuvent mieux percevoir les contraintes qu'il fait peser sur elles, mais il demeure sur de nombreux points encore insuffisamment clair, et sans doute encore inadapté aux enjeux mondiaux.

2. La réponse du politique

M. André SANTINI
Député, Maire d'Issy-les-Moulineaux

Mme. Meryem MARZOUKI
Président directeur général de LaSer et de Cofinoga, membre de la CNIL

M. André SANTINI
Député, Maire d'Issy-les-Moulineaux

Depuis plus de cinq ans, je milite pour l'introduction du vote par Internet dans notre code électoral. C'est parce qu'il s'agit d'un sujet controversé que j'ai lancé, à cette époque, le Forum Mondial de l'e-Démocratie. Je voulais inviter les responsables

étrangers qui travaillent sur le sujet pour contribuer à faire avancer notre propre réflexion sur le sujet.

Je reviens d'une mission en Corée du Sud : les Coréens ont adopté un plan d'action qui prévoit, dès 2008, la possibilité de voter, à partir de machines à voter, depuis n'importe quel bureau de vote installé dans le pays.

Les personnes handicapées et les Coréens de l'étranger (800.000 personnes sont concernées) pourront, quant à eux, voter en ligne, à partir d'un PC, d'un téléphone mobile ou d'un PDA sans avoir besoin de se rendre dans un bureau de vote. Ce système serait ensuite généralisé à tous les électeurs aux élections générales de 2012.

D'ici là, les autorités coréennes travailleront sur les questions que tous les pays se posent sur le vote par Internet : sécurité et anonymat du vote notamment.

C'est une méthode radicalement différente de celle que nous privilégions en France. Ici, on a commencé par dire : « impossible », puis « on verra », puis « pourquoi pas ? ». On débat et on discute, mais aucune étude, aucune expérience, aucun plan national n'est à l'ordre du jour. On attend, alors que nous pourrions au moins tenter de répondre aux principales questions que posent le vote par Internet et, plus largement d'ailleurs, le vote à distance.

Nous pouvons aujourd'hui bénéficier de plusieurs expériences qui ont été menées en Grande Bretagne, en Suisse et en Estonie.
Que démontrent-elles ? En Suisse, le Centre d'études et de documentation sur la démocratie directe de l'Université de Genève a analysé le comportement des électeurs du canton de Genève :

1. Sans vote par Internet, les jeunes seraient sous-représentés parmi les votants. Le vote par Internet a augmenté la proportion des jeunes votants (entre 18 et 29 ans). Les moins de 30 ans forment entre 10 et 12% de l'électorat, mais ne représentent généralement que 5 % des suffrages exprimés. Avec Internet, la proportion des jeunes votants est remontée au niveau de leur poids démographique.

2. Internet a davantage déplacé des électeurs habituels vers un nouveau mode d'expression qu'il n'a bouleversé le taux de participation, sauf justement chez les jeunes.

3. La participation semble subir un petit coup de pouce, même s'il y a surtout un effet de report du vote par correspondance sur le vote par Internet. Entre 12 et 16 % des votants par Internet sont des votants occasionnels ou abstentionnistes, et affirment qu'ils participeraient plus facilement à des scrutins si le e-voting était généralisé.

4. Enfin, plus un individu utilise internet, plus il a confiance dans la procédure et plus il est favorable à la généralisation du vote électronique en complément des possibilités déjà existantes.

En Estonie, 1er pays à avoir légiféré pour autoriser le vote par Internet aux élections municipales qui ont eu lieu il y a trois semaines, près de 10.000 électeurs, soit 1% du corps électoral, ont voté par ce biais sans rencontrer de difficultés.

La procédure de vote était simple : les Estoniens avaient besoin d'une Carte d'Identité Electronique, d'un ordinateur connecté et d'un lecteur de carte. Après avoir été authentifiés par leur Carte d'identité électronique, ils pouvaient faire leur choix et l'envoyer sur un serveur sécurisé. Ils devaient ensuite confirmer leur vote en saisissant un code PIN. Environ 60 % des Estoniens ont une carte d'identité électronique, utilisée depuis 2002 pour l'accès en ligne aux comptes bancaires ou aux services fiscaux. Mais beaucoup d'utilisateurs ne disposent pas d'un lecteur de carte à la maison, ce qui explique la faible participation du vote en ligne.

En France, la situation est confuse :

- **Nous assistons, d'une part, au développement des machines à voter**.

Mais elles sont coûteuses (plus de 500.000 euros si nous remplaçons chaque isoloir par une machine à voter dans les bureaux de vote d'Issy-les-Moulineaux).

Elles soulageraient le personnel des bureaux de vote sans rendre service aux électeurs.

Elles posent les mêmes questions de sécurité et de fiabilité que le vote par Internet.

- **Nous assistons**, d'autre part, au développement du **vote par Internet pour des élections professionnelles**, lors **d'assemblées générales d'entreprises**, de **délégués du personnel**, de **congrès de partis politiques** (cf. UMP), aux **chambres de commerce et d'industrie**, ou **chez les avocats**.

Maintenant que des milliers de Français ont pu voter par Internet, nous entendons les opposants au système faire une distinction, quasi méprisante, entre les élections politiques, trop sérieuses pour qu'on teste l'e-vote, et les autres.

Pourtant, c'est bien par l'Internet que les Français installés aux États-Unis ont élu, en 2003, leurs représentants au Conseil Supérieur des Français de l'Etranger. Et c'est bien sur la généralisation du système à l'ensemble des Français de l'étranger que le gouvernement travaille pour les élections présidentielles de 2007.

La question n'est donc plus de savoir si nous voterons par Internet, mais pour quelle élection et quand ?

Avant d'envisager une généralisation à tous les scrutins politiques et pour tous les électeurs, nous pourrions commencer par un système mixte, tel que celui expérimenté à Issy-les-Moulineaux lors du référendum du 29 mai dernier par le Ministère de l'Intérieur, dans le cadre du projet européen e-Poll.

Il s'agissait de machines à voter en réseau. Si le Ministère de l'Intérieur modifie le code électoral, comme il l'a annoncé lors du dernier Forum Mondial de l'e-Démocratie, ces machines permettraient à n'importe quel électeur de voter depuis un bureau de vote situé n'importe où sur le territoire.

Ce serait un premier pas, mais encore insuffisant à mes yeux.

Pourquoi le vote par Internet ?

Promouvoir le vote par Internet ne répond pas seulement à la nécessité d'adapter notre vie politique à une époque où nous gérons nos comptes bancaires et payons nos impôts en ligne.

Il s'agit aussi, et peut être surtout, d'essayer de lutter contre la montée de l'abstention. Depuis vingt ans, nous subissons sans réagir une désaffection de plus en plus grande de nos concitoyens dans les principaux rendez-vous électoraux.

Si vous prenez les différents scrutins qui ont eu lieu en 2004 : élections régionales, cantonales et européennes, vous constaterez qu'un Français sur quatre, inscrit sur les listes électorales, s'est abstenu de voter à toutes les élections organisées sur l'année. Ce chiffre marque une forte progression de « l'abstentionnisme systématique » pour reprendre la formule des experts. 85 % de ceux qui n'ont pas voté en 2004 s'étaient déjà abstenus à tous les scrutins de 2002.

Mais le plus inquiétant, c'est que seuls 40 % des jeunes adultes (20-29 ans) ont voté alors que ce taux atteint près de 70 % dans la tranche des 60-69 ans. Comment peut-on alors parler de légitimité ?

Cependant, les choses avancent : l'environnement juridique autour du vote par Internet se met progressivement en place.

La délibération de juillet 2003 de la CNIL, suivie, en septembre 2004, d'une recommandation des 46 pays membres du Conseil de l'Europe visant à garantir l'équité d'un vote électronique, insistent sur les normes juridiques, opérationnelles et techniques à mettre en œuvre pour assurer un scrutin équitable et fiable.

La recommandation du Conseil de l'Europe constitue une base européenne légale au vote électronique et doit permettre à tous les acteurs d'avancer.

Le 3 octobre dernier, la cour d'appel de Lyon a délivré un arrêt, suite à la plainte d'un candidat malheureux aux élections du Barreau de Paris qui demandait l'annulation des élections de novembre 2004 en estimant que les conditions dans lesquelles étaient organisées le vote par Internet ne présentaient pas de garanties suffisantes de respect des principes généraux du droit électoral, ni le secret du vote, ni son caractère personnel.

Dans son arrêt, la Cour a conclu qu'il n'existait « aucun motif sérieux de nature à mettre en doute la régularité des opérations électorales, la parfaite information des électeurs, leur liberté de choix, le secret du vote et la sincérité du scrutin ».

Cette jurisprudence confirme que le vote par Internet est possible en France. Il s'agit d'une question de volonté politique.

Mais nous devons répondre aux inquiétudes et aux questions qui s'expriment autour du vote par Internet.

- **voter à distance ne dévalorise t-il pas l'acte républicain** qui consiste à se déplacer dans le **bureau de vote pour exercer son devoir**.

Je suis, pour ma part, partisan du libre choix de la procédure de vote pour l'électeur. En élargissant les modalités de vote, nous offrons aux électeurs empêchés (hospitalisation, handicap, déplacements) la possibilité d'exercer leurs droits civiques.

Et personne ne prétendra, aujourd'hui, que le vote par Internet va supprimer les bureaux de vote.

- **Comment assurer l'identification de l'électeur ?**

C'est un vrai débat qu'il faut mener : faut-il utiliser la carte d'identité électronique, comme en Estonie, ou expédier par la poste une carte d'électeur qui comporte une case à gratter, contenant identifiant et mot de passe, comme à Genève ?

C'est cette dernière procédure que nous avons choisi à Issy-les-Moulineaux pour les élections par Internet de nos conseils de quartier qui auront lieu en décembre prochain : l'électeur reçoit sa carte électorale et ses codes d'identification sont cachés sous une case à gratter. Il est ainsi le seul à pouvoir les découvrir.

- **Comment garantir l'absence de pression sur le vote ?**

Dans un pays qui ne propose pas le vote par correspondance, la question du vote sous influence se pose évidemment.

Nul ne doute pourtant du caractère démocratique de ceux qui, comme l'Allemagne ou la Suisse, autorisent le vote par correspondance.

Pour y remédier, pourquoi ne pas s'inspirer du modèle Estonien ? Tout électeur votant par Internet a le droit de se rendre dans son bureau de vote, le jour du scrutin. Dans ce cas, son vote en ligne est annulé au bénéfice de son vote papier. C'est aussi ce que fait la Norvège dans le cadre du vote par correspondance. Cela ôte tout soupçon de vote sous pression.

- **Comment assurer la transparence du contrôle des opérations électorales ?**

Aujourd'hui, tout électeur peut assister et contrôler le dépouillement des votes papier. Cela ne sera plus possible avec le vote électronique, que ce soit sur machine ou sur Internet.

Le contrôle pourrait être assuré par un organisme officiel doté d'experts capables de réaliser des audits, avant, pendant et après les opérations de vote. Cela peut aussi passer par l'utilisation de logiciels en open source, permettant ainsi d'accéder aux codes sources du système.

Nous avons, nous, responsables politiques, un vrai effort à faire pour assurer la transparence des opérations de vote et pour créer une nouvelle chaîne de confiance dans le processus électoral numérique. **Lorsqu'il s'agira de légiférer** sur la question, **nous devrons adopter des dispositions pour décourager et punir ceux qui tenteraient de fausser les résultats des scrutins, notamment pour empêcher :**

- l'achat, le vol, le refus d'accorder une signature électronique dans un but frauduleux
- les contraintes sur un électeur
- les attaques des systèmes de vote ou d'un vote individuel
- le blocage d'un système de vote par la réduction ou l'élimination des accès au système des électeurs qui désireraient prendre part à une élection par Internet
- l'envoi abusif d'informations sur un système de vote dans le but de réduire la capacité des organisateurs d'une élection à répondre aux demandes des électeurs
- l'ingérence dans la vie privée en attaquant un vote ou un site avec l'intention de connaître le vote exprimé ou de changer le vote.

L'e-démocratie ne se résume pas au vote par Internet. Celui-ci ne règlera pas non plus la crise de défiance que traverse la vie politique française depuis 25 ans, mais il symbolisera la capacité des élus à s'adapter au monde moderne et à un mode de vie qui séduit de plus en plus de Français.

Mme. Meryem MARZOUKI
Chercheur au laboratoire LIP6/PolyTIC-CNRS
Présidente de l'association IRIS

Si l'on veut se préoccuper du cadre juridique en matière de protection des données personnelles dans sa globalité, il faut tout d'abord rappeler qu'entre l'adoption de la loi Informatique et Libertés en 1978 et sa révision en 2004[1], toute une série de mesures ont été adoptées.

Notes

[1] Loi n°2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, disponible à <http://www.legifrance.gouv.fr/WAspad/UnTexteDeJorf?numjo=JUSX0100026L>

Pour n'en citer que quelques unes, rappelons la loi sur la vidéosurveillance de 1995[1] ; la loi sur la sécurité quotidienne de 2001[2] (dont les dispositions sur la rétention des données de télécommunication étaient déjà présentes dans le projet de loi sur la société de l'information de 1999[3]) ; la loi sur la sécurité intérieure en 2003[4] également, qui a permis l'extension du fichier national automatisé des empreintes génétiques (FNAEG) ; la loi sur l'immigration en 2003[5] (autorisant l'usage de la biométrie dans les visas et pour les contrôles aux frontières).

On peut y ajouter, après la révision de la loi Informatique et Libertés elle-même, le projet INES[6] de carte d'identité biométrique et le projet de loi de lutte contre le terrorisme[7], qui vise à généraliser la vidéosurveillance, la rétention de données et l'usage des dossiers passagers détenus par les compagnies aériennes, maritimes et ferroviaires.

De plus, cette activité législative et réglementaire se poursuit dans un contexte européen et international qui a provoqué des modifications importantes du cadre juridique.

Si l'on analyse assez globalement cette évolution, on constate certaines caractéristiques indiquant un changement en profondeur, qui se traduit par trois éléments :

1. L'État cède de ses prérogatives au profit de certains acteurs privés, leur délégant ainsi une part de ses pouvoirs régaliens.
2. Dans le même temps, l'État consolide sa propre logique policière, en s'affranchissant des contrôles citoyens, notamment ceux qui peuvent être exercés au travers de la CNIL.
3. Tout cela se déroule dans un contexte de consentement assez généralisé, bien que quelques voix continuent de s'élever.

---

[1] *Loi n°95-73 du 21 janvier 1995 d'orientation et de programmation relative à la sécurité, disponible à <http://www.legifrance.gouv.fr/WAspad/UnTexteDeJorf?numjo=INTX9400063L>*

[2] *Loi n°2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne, disponible à <http://www.legifrance.gouv.fr/WAspad/UnTexteDeJorf?numjo=INTX0100032L>*

[3] *Projet de loi, transmis au Parlement le 18 juin 2001, sur la société de l'information, disponible à <http://www.assemblee-nationale.fr/projets/pl3143.asp>*

[4] *Loi n°2003-239 du 18 mars 2003 pour la sécurité intérieure, disponible à <http://www.legifrance.gouv.fr/WAspad/UnTexteDeJorf?numjo=INTX0200145L>*

[5] *Loi n°2003-1119 du 26 novembre 2003 relative à la maîtrise de l'immigration, au séjour des étrangers en France et à la nationalité, disponible à <http://www.legifrance.gouv.fr/WAspad/UnTexteDeJorf?numjo=INTX0300040L>*

[6] *Projet de programme INES (Identité nationale électronique sécurisée) du ministère de l'Intérieur, 1er mars 2005, disponible à <http://www.foruminternet.org/telechargement/forum/pres-prog-ines-20050301.pdf>*

[7] Projet de loi, transmis au Parlement le 25 octobre 2005, relatif à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers, dossiers sur le site de l'Assemblée nationale <http://www.assemblee-nationale.fr/12/dossiers/terrorisme_securite_controles.asp> et du Sénat <http://www.senat.fr/dossierleg/pjl05-109.html>

J'essaierai de développer ces trois points à l'aide de quelques exemples dans la suite de mon intervention, avant de conclure sur les implications en termes de respect de l'État de droit et du contrat social entre l'État et le citoyen.

Un transfert de pouvoirs régaliens à des acteurs privés

La nouvelle loi Informatique et Libertés n'innove pas en termes de transfert des prérogatives de l'État au profit de certains acteurs privés. Pour rester dans le secteur de l'informatique et des réseaux numériques, la loi pour la confiance dans l'économie numérique[1], adoptée quelques semaines auparavant, permettait déjà à l'État de céder à des intermédiaires techniques certaines prérogatives de contrôle jusque-là réservées à l'autorité judiciaire. Toutefois, la nouvelle loi Informatique et Libertés comporte des dispositions qui consacrent ce phénomène et lui donnent plus d'ampleur.

Il en est ainsi de l'article 9 de la nouvelle loi Informatique et Libertés, partiellement censuré par le Conseil constitutionnel. Cet article autorise en effet les sociétés de gestion des droits de propriété intellectuelle à mettre en oeuvre des traitements de données relatives aux infractions, condamnations et mesures de sûreté. Rappelons que cette disposition n'est pas une obligation découlant de la transposition de la Directive européenne de 1995. Ces acteurs privés deviennent ainsi autorisés à tenir ce que plusieurs organisations, réunies au sein de l'intercollectif Droits et libertés face à l'informatisation de la société (DELIS[2]), avaient qualifié de « véritables casiers judiciaires privés », et sont transformés en « forces de l'ordre *sui generis* », selon les termes employés par l'opposition parlementaire dans sa saisine du Conseil constitutionnel[3].

Plus largement, l'article 8-II de cette même loi prévoit des exceptions supplémentaires au principe interdisant la collecte de données sensibles, avec notamment une exception motivée par « les traitements nécessaires à la constatation, à l'exercice ou à la défense d'un droit en justice », formulation qui, sans limite d'interprétation, peut couvrir par exemple des activités de la vie d'une entreprise.

Certes, la CNIL a refusé, dans une délibération récente[4], d'autoriser des sociétés d'auteur à mettre en oeuvre des dispositifs de détection automatisée des infractions au code de la propriété intellectuelle et l'envoi de messages aux internautes concernés, au nom du respect des principes de finalité et de proportionnalité, ainsi que du nécessaire contrôle de l'autorité judiciaire. Mais la CNIL pourra-t-elle encore exercer ce contrôle, alors même que certains articles de presse[5] mentionnent des velléités de modification législative dans le cadre du projet de loi sur le droit d'auteur

---

[1] Loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, disponible à <http://www.legifrance.gouv.fr/WAspad/UnTexteDeJorf?numjo=ECOX0200175L>

[2] <http://www.delis.sgdg.org>

[3] <http://www.conseil-constitutionnel.fr/decision/2004/2004499/saisine1.htm>

[4] « Peer to peer : la CNIL n'autorise pas les dispositifs présentés par les sociétés d'auteurs et de producteurs de musique » (18 octobre 2005. Voir <http://www.cnil.fr/index.php?id=1881&news%5Buid%5D=284&cHash=dd58aa6ed2>

[5] Cf. par exemple un article de VNUnet.fr du 26 octobre 2005, disponible à <http://www.vnunet.fr/actualite/tpepme_-_business/vie_publique/20051026007>

et les droits voisins dans la société de l'information, pour éviter que la CNIL puisse poursuivre sa mission ?

Une logique policière affranchie du contrôle citoyen

Cet affranchissement du contrôle citoyen exercé à travers la CNIL est à l'œuvre depuis plusieurs années, concernant non pas les acteurs privés mais l'État lui-même, qui a consolidé peu à peu une logique policière.

Tout d'abord, cet affranchissement a procédé par l'adoption de mesures législatives plutôt que réglementaires, permettant d'échapper à des objections éventuelles de la CNIL en ne lui accordant qu'un avis consultatif. Avec la loi de 1995 par exemple, la vidéosurveillance échappe à la nécessité d'un accord de la CNIL, du moins dans les lieux publics. Il en va de même de la création de certains grands fichiers de police judiciaire ou administrative.

Mais, depuis l'adoption de la nouvelle loi Informatique et Libertés, il n'est même plus nécessaire de recourir à des mesures législatives pour contourner le contrôle de la CNIL.
En effet, les articles 26 et 27 de cette nouvelle loi suppriment le véritable « droit de veto » dont la CNIL bénéficiait jusqu'alors par la nécessité de prendre des mesures réglementaires par décret sur avis conforme du Conseil d'État. Cette suppression est effective, y compris en cas de traitement de données sensibles, de traitement du NIR (numéro de sécurité sociale dont on sait combien il est signifiant et historiquement marqué), et même de traitement de données biométriques.

On observe déjà les conséquences de cet affranchissement de l'accord de la CNIL avec deux décrets concernant la délivrance de visas à des ressortissants étrangers, l'un datant de novembre 2004[1], l'autre d'août 2005[2] et portant plus spécifiquement sur le traitement automatisé des demandes de validation d'attestation d'accueil pour l'obtention de visas de court séjour. Dans les deux cas, de nombreuses réserves de la CNIL[3] n'ont pas été suivies par l'État, et le deuxième décret fait d'ailleurs l'objet

---

[1] *Décret n°2004-1266 du 25 novembre 2004 pris pour l'application de l'article 8-4 de l'ordonnance n° 45-2658 du 2 novembre 1945 relative aux conditions d'entrée et de séjour des étrangers en France et portant création à titre expérimental d'un traitement automatisé des données à caractère personnel relatives aux ressortissants étrangers sollicitant la délivrance d'un visa, disponible à <http://www.legifrance.gouv.fr/WAspad/UnTexteDeJorf?numjo=INTD0400325D >*

[2] Décret n°2005-937 du 2 août 2005 pris pour l'application de l'article L. 211-7 du code de l'entrée et du séjour des étrangers et du droit d'asile et portant sur le traitement automatisé de données à caractère personnel relatif aux demandes de validation des attestations d'accueil, disponible à <http://www.legifrance.gouv.fr/WAspad/UnTexteDeJorf?numjo=INTD0500214D >

[3] *Respectivement : Délibération n°2004-075 du 5 octobre 2004 portant avis sur le projet de décret en Conseil d'État pris pour l'application de l'article 8-4 de l'ordonnance du 2 novembre 1945 relative aux conditions d'entrée et de séjour des étrangers en France et portant création à titre expérimental d'un traitement automatisé de données à caractère personnel relatives aux ressortissants étrangers sollicitant la délivrance d'un visa (demande d'avis n°1034770), disponible à <http://www.legifrance.gouv.fr/WAspad/UnTexteDeJorf?numjo=CNIX0407821X> et Délibération n°2005-052 du 30 mars 2005 portant avis sur le projet de décret en Conseil d'État prévu par l'article*

d'un recours devant le Conseil d'État, présenté conjointement par le Groupe d'information et de soutien des immigrés (GISTI[1]), la Ligue des droits de l'Homme (LDH[2]) et l'association Imaginons un réseau Internet solidaire (IRIS[3]). Le projet de loi relatif à la lutte contre le terrorisme, qui sera bientôt discuté au Parlement, renvoie l'application de plusieurs de ses dispositions importantes à des décrets en Conseil d'État, une procédure qui, de la même façon, ne laisse à la CNIL qu'un rôle consultatif.

Un climat de consentement social

Le plus étonnant reste que tous ces développements se déroulent dans une atmosphère de consentement assez généralisé, qui tranche par rapport au véritable scandale public qu'avait provoqué, il y a plus de 30 ans, la révélation par la presse du projet SAFARI[4]. Ce scandale a donné lieu quatre années plus tard à l'adoption de la première loi Informatique et Libertés en 1978, l'une des premières lois de protection de la vie privée et des données personnelles en Europe, et à la création de la CNIL. Que s'est-il donc passé entre-temps ?

L'émergence d'une « culture de la sécurité »

Tout d'abord, une véritable « culture de la sécurité » s'est installée peu à peu, et singulièrement une « culture de la cybersécurité » pour reprendre les termes de la Déclaration adoptée dans le cadre du Sommet mondial sur la société de l'information (SMSI) par les États membres des Nations Unies[5]. Il est donc intéressant d'explorer plus en profondeur cette véritable « fabrique du consentement » à toujours plus de mesures attentatoires aux droits fondamentaux et aux libertés. On peut en trouver certains fondements dans le discours politique destiné à justifier des mesures de plus en plus sécuritaires, et l'exemple des principaux arguments avancés pour justifier le projet INES est, à cet égard, édifiant.

Ce discours se caractérise par quatre arguments principaux destinés à légitimer les mesures sécuritaires : la lutte contre toutes sortes de fraudes ; les obligations internationales à respecter ; l'efficacité et la rationalisation des procédures ; le caractère conjoncturel et donc provisoire des mesures d'exception.

L. 211-7 du code de l'entrée et du séjour des étrangers et du droit d'asile et relatif aux modalités de mise en oeuvre par les maires, agissant en leur qualité d'agents de l'État, d'un traitement automatisé de données à caractère personnel relatif aux demandes de validation des attestations d'accueil (demande d'avis n° 1 046 585), disponible à <http://www.legifrance.gouv.fr/WAspad/UnTexteDeJorf?numjo=CNIL0508651X>

[1] *<http://www.gisti.org>*

[2] *<http://www.ldh-france.org>*

[3] *<http://www.iris.sgdg.org>*

[4] *Le projet SAFARI (Système Automatisé pour les Fichiers Administratifs et le Répertoire des Individus) a été révélé par un article du journal* Le Monde *daté du 21 mars 1974 et intitulé « SAFARI ou la chasse aux Français ».*

[5] *Formule employée au paragraphe 35 de la Déclaration de Genève, adoptée lors de la première phase du Sommet en décembre 2003, disponible à <http://www.itu.int/wsis/docs/geneva/official/dop-fr.html> et réaffirmée au paragraphe 39 de l'*Agenda de Tunis*, adopté lors de la deuxième phase du Sommet en novembre 2005, disponible à <http://www.itu.int/wsis/docs2/tunis/off/6rev1-fr.html>*

Le premier argument utilisé est que les documents actuels d'identité et de voyage ne seraient pas sécurisés, et permettraient une fraude de grande ampleur. Or, le ministère de l'Intérieur a lui-même reconnu que des évaluations chiffrées de cette fraude n'étaient pas disponibles. Cela n'a pas empêché le développement d'un discours fondé sur la nécessité d'empêcher, au moyen de documents plus sécurisés grâce à la biométrie, l'immigration illégale, le bénéfice indu de prestations médicales et sociales, voire la fraude fiscale. Le message est clair : l'honnête consommateur et contribuable, à qui ce discours est d'ailleurs adressé, serait la première victime de telles fraudes : il faut donc l'en protéger.

De plus, les réglementations internationales nous imposeraient la mise en place de ce projet. Il est fait notamment référence aux standards établis par l'Organisation de l'aviation civile internationale (OACI[1]) et au Règlement du Conseil européen adopté en décembre 2004 en matière de passeports biométriques[2]. Cet argument passe sous silence à la fois le fait que ces deux réglementations ne concernent que les passeports, et non les documents nationaux d'identité et le fait que le standard de l'OACI ne rend obligatoire que l'utilisation de la photo numérisée, et non les empreintes digitales en tant qu'élément biométrique. Enfin, il édulcore la réalité du fonctionnement d'instances intergouvernementales telles que l'OACI et, a fortiori, le Conseil européen : la France, tout comme les autres États, y est bien représentée, et capable d'y faire entendre sa voix. Présenter comme une obligation subie la mise en place de décisions politiques internationales ou régionales auxquelles la France a participé, parfois avec un rôle promoteur, constitue ce que certaines organisations non gouvernementales ont qualifié de « blanchiment de politique ».

En outre, les arguments sécuritaires en faveur du projet de carte d'identité biométrique ont été appuyés par des avantages escomptés en termes de développement de l'administration électronique et des transactions électroniques marchandes, qui seraient facilitées par une meilleure authentification de la signature. Un tel discours tend à privilégier des objectifs d'efficacité et de rationalisation des méthodes et procédures sur les principes cardinaux de la protection de la vie privée et des données personnelles que sont les principes de proportionnalité et de finalité. Il entérine de plus, et par avance, les extensions, voire les détournements de finalité qui pourraient suivre l'adoption du principe de l'utilisation de la biométrie pour l'authentification et l'identification, tout comme les finalités de certains fichiers ont été étendues au cours du temps. On peut citer à cet égard le cas emblématique du FNAEG qui, du fichage des auteurs de crimes sexuels à sa création en 1998, en est progressivement arrivé à concerner toute personne convaincue, ou seulement suspectée, d'un simple délit contre les biens ou les personnes.

Enfin, au-delà du projet INES, le recours à des « clauses de rendez-vous » est de plus en plus fréquent dans la législation, afin de rassurer et apaiser d'avance des critiques qui se feraient trop vives. C'était le cas pour plusieurs dispositions de la loi sur la

---

[1] *<http://www.icao.int>*

[2] *Règlement (CE) n°2252/2004 du Conseil du 13 décembre 2004 établissant des normes pour les éléments de sécurité et les éléments biométriques intégrés dans les passeports et les documents de voyage délivrés par les États membres, disponible à <http://europa.eu.int/eur-lex/lex/LexUriServ/LexUriServ.do?uri=OJ:L:2004:385:0001:0006:FR:PDF >*

sécurité quotidienne, c'est également le cas dans le projet de loi relatif à la lutte contre le terrorisme. De telles « clauses de rendez-vous » servent à justifier une législation d'exception, censée être révisée dès que le danger auquel elle fait face se sera atténué ; elles ont été également utilisées à l'étranger, par exemple aux États-Unis avec les *Patriot Act Sunsets*[1]. Il s'est avéré que, dans le cas de la loi sur la sécurité quotidienne, les dispositions concernées ont été pérennisées avant même l'expiration du délai fixé. De surcroît, les évaluations qui devaient permettre la décision de réexamen n'ont tout simplement pas été conduites.

L'érosion du sens de la vie privée

Pour autant, l'utilisation du « sentiment d'insécurité » et plus généralement le jeu sur les angoisses légitimes provoquées par les attentats du 11 septembre 2001 aux États-Unis et ceux qui ont suivi, notamment en Europe, ne sont pas les seuls éléments qui ont conduit à la généralisation du consentement dans la société. La société technicienne n'a cessé d'être théorisée, analysée et critiquée depuis près d'un demi-siècle. Toutefois, jamais encore le sens de la vie privée des individus n'avait été autant affecté, pour en arriver à un tel degré de consentement au contrôle. Ce phénomène peut sans doute être expliqué par la conjonction de quatre facteurs : la banalisation de l'usage des techniques ; la recherche du confort maximal ; la marchandisation du corps et de l'intimité ; la perte de conscience d'un contrôle devenu banalisé et indolore.

Parler de banalisation de l'usage des techniques relèverait presque du lieu commun, tant le phénomène d'appropriation des techniques d'information et de communication est réel, tous médias confondus, dans toutes les sphères de l'activité humaine, publique ou privée, professionnelle ou personnelle. Dans ce contexte, le dispositif technique apparaît plus comme un instrument indispensable que comme un moyen de contrôle des activités de l'individu. Ce dispositif devient domestiqué au point qu'il ne saurait plus représenter un danger – quand il n'est pas carrément partie de l'univers affectif de l'individu, comme l'ont montré des études sur les usages des téléphones portables. Son fonctionnement maîtrisé, le dispositif technique est même perçu au contraire comme un élément de filtrage *par* l'individu des accès à son espace, à ses informations et à ses biens (puisqu'il en possède ou connaît les codes d'entrée ou d'accès), voire à sa personne (puisqu'il peut gérer sa disponibilité), en fonction de ses propres choix. Il est enfin un moyen de surveillance et de contrôle exercé par l'individu lui-même, par exemple par l'usage d'outils de contrôle parental ou de caméras de surveillance domotique. Outre un phénomène d'appropriation de la technique elle-même, il y a donc un effet d'appropriation du contrôle au moyen de la technique qui doit être considéré.

L'argument de confort vient souvent compléter la présentation des nombreux avantages de l'utilisation des techniques d'informatisation ou de biométrie. Gain de temps, allègement des procédures, diminution des encombrements, « moins de papiers » à présenter ou à transporter, sont autant de justificatifs fournis à l'appui d'un consentement au contrôle numérisé. Ces arguments sont très présents dans les

[1] *Voir à ce sujet la page qu'y consacre l'*American Civil Liberty Union, *disponible à <http://action.aclu.org/reformthepatriotact/sunsets.html>*

discours des prescripteurs. S'agissant du développement de l'administration électronique, par exemple, le « guichet unique » à disposition de l'usager ou encore les « formulaires pré-renseignés », figurent parmi les principales caractéristiques mises en avant pour le grand public. On a pu également entendre un maire justifier, au cours d'une conférence publique[1], le « portfolio personnel » associé à la carte d'identité biométrique dans le projet INES, par l'avantage qu'il y aurait à ne transporter sur soi qu'une seule carte au lieu de plusieurs. Mais ces avantages valent aussi pour les usagers ou les consommateurs. Ainsi, au cours d'un reportage télévisé[2] sur l'expérience « Pégase[3] » de contrôle biométrique pour le passage des frontières à l'aéroport de Roissy-Charles de Gaulle, un usager témoignait de l'aspect « rapide et ludique » de ce procédé de contrôle[4].

Un troisième phénomène est à l'œuvre, dans le prolongement des transformations sociales mais plus particulièrement à la rencontre de la technique et des mécanismes de marché, et donne lieu à une marchandisation du corps et de l'intimité. Le commerce électronique des biens et des services a consacré le développement de techniques de marketing nouvelles, pour lesquelles des profils quasi-individualisés de consommateurs ont largement supplanté l'identification de tendances et catégories génériques de consommation dans une population cible. De tels profils affinés requièrent la connaissance de données personnelles, voire intimes, qui constituent par conséquent une valeur marchande importante. Le consommateur en a vite lui-même compris la réalité, et a également développé des stratégies pour se protéger mais aussi pour utiliser à son profit cette valeur marchande. Certaines stratégies de protection font usage de logiciels de filtrage permettant la maîtrise des données personnelles collectées par certains sites web[5]. Les stratégies d'utilisation sont toutes fondées sur le même principe : le consommateur accepte de fournir des informations personnelles, ou accepte une intrusion dans son intimité, pour obtenir en contrepartie un avantage directement marchand (bénéfice « gratuit » ou réduction de coûts d'accès à un service) ou, plus subtilement, le sentiment d'appartenance à un groupe privilégié (effet « club » des formules de fidélisation de clientèle). Dans tous les cas, la base de ces stratégies est le postulat que la vie privée est négociable, au même titre que la propriété, et leur fonctionnement est fondé sur la mise en œuvre d'un échange marchand, dans lequel le consommateur consentant troque des aspects de sa vie privée ou de son intimité contre le bénéfice d'un bien ou d'un service. La question de la maîtrise des données personnelles envisagée comme l'exercice d'un droit de propriété avait déjà suscité certaines interrogations à propos du développement de l'administration électronique[6]. Sachant que le consentement individuel constitue le

---

[1] Journée de l'Association des Maires des Grandes Villes de France. « Une carte ou des cartes ? ». 9 juin 2005. Paris

[2] Journal télévisé sur la chaîne France 2

[3] Cf. présentation de cette expérience sur le site d'Air France, disponible à <http://www.airfrance.fr/cgi-bin/AF/FR/fr/local/guidevoyageur/e_services/e_services_pegase.htm>

[4] Lire à cet égard les conclusions du rapport de recherche INT « La biométrie, usages et représentations », publié en février 2004 (auteurs : Sylvie Craipeau, Gérard Dubey, Xavier Guchet), disponible à : <http://www.int-evry.fr/biometrics/downloads/proReports/rep4072e21a2b224.doc>

[5] Comme par exemple la plate-forme P3P (Privacy Preferences Protection) développée par le W3C.

[6] Voir à ce sujet un chapitre du « Livre vert sur l'administration électronique et les données personnelles », publié en février 2002 en conclusion de la mission confiée à Pierre Truche, Jean-Paul

fondement de nombre de mesures législatives en matière de protection de la vie privée et des données personnelles, il conviendrait sans doute de tirer les conséquences de ce phénomène de négociation marchande qui met en péril le droit à la vie privée en tant que droit fondamental inaliénable.

Enfin, il est d'autant plus difficile de résister au contrôle que l'on en perd la conscience, lorsqu'il devient banalisé et indolore. Or l'usage de dispositifs techniques pour le contrôle aboutit justement à un tel résultat, pour trois raisons. D'abord, le dispositif technique agit comme médiateur de la procédure, tenant le contrôleur humain – en particulier le policier – à une distance telle qu'il n'apparaît plus nécessairement face au contrôlé, son action s'effectuant à distance, et parfois en différé, par la consultation des données recueillies ; c'est en particulier le cas avec les contrôles biométriques, la vidéosurveillance, etc. Ensuite, le procédé technique employé ne permet pas toujours à la personne contrôlée de se rendre compte qu'il y a contrôle et recueil de données ; ainsi, les dispositifs utilisant des puces RFID, de même que les techniques de biométrie « à traces » (par exemple empreintes digitales, mais aussi reconnaissance faciale puisque des photographies peuvent être prises à la volée) permettent le contrôle à l'insu de la personne concernée. Enfin, le net glissement législatif (au niveau national ou européen) d'un contrôle ciblé par conservation des données concernant une personne particulière faisant l'objet d'une investigation judiciaire vers un contrôle systématique de tous par la rétention généralisée des données fait de la suspicion la règle et non plus l'exception ; il devient alors « normal » de faire l'objet d'une surveillance et d'un contrôle constant.

Des brèches dans le contrat social

En résumé, l'évolution du cadre juridique et du contexte national, européen et international en matière de protection de la vie privée et des données personnelles est caractérisée par un transfert de prérogatives régaliennes de l'État vers des acteurs privés, par une diminution des possibilités de contrôles citoyens, et par un climat de consentement social qui dilue toute résistance.

Au terme de cette rapide analyse, on ne peut que faire le constat que l'État de droit devient affecté par cette évolution, qui restreint sévèrement la possibilité de contrôle démocratique et l'accès à des voies de recours, autorisant ainsi les mesures arbitraires, parfois en l'absence de toute transparence lorsqu'elles sont mises en oeuvre par des acteurs privés.

Au-delà de la seule question de la protection de la vie privée et des données personnelles, c'est le socle même du contrat social qui devient entamé. Les modifications dans la perception de l'identité, avec l'introduction des contrôles biométriques, opèrent une transformation profonde qui, de déclarative et fondée sur la confiance et la reconnaissance mutuelles, devient réifiée et intangible[1]. L'inversion

---

Faugère et Patrice Flichy, disponible à <http://www.ladocumentationfrancaise.fr/rapports-publics/024000100/index.shtml>

[1] *Comme le relevait l'argumentaire du collectif pour le retrait du projet INES, disponible à <http://www.ines.sgdg.org/article.php3?id_article=13>*

des valeurs devient totale en conséquence d'un climat de suspicion généralisée et de la transformation de la présomption d'innocence en une présomption de culpabilité.

Au final, ce sont donc les relations de pouvoir entre les citoyens et l'État qui sont durablement et profondément transformées par l'imposition d'un tel contrôle devenu routinier, et perçu comme tel.

3. La réponse de l'ordre public

M. François JASPART
Directeur de la police judiciaire à la Préfecture de police de Paris

M. François GIQUEL
Conseiller maître à la Cour des Comptes, vice-Président de la CNIL

M. François JASPART

Directeur de la police judiciaire à la Préfecture de police de Paris

Avant de répondre à la question posée par ce colloque, en ma qualité de représentant de la force publique dont une des missions est la préservation de l'Ordre Public, il est important, pour la clarté de l'exposé, de rappeler rapidement quelques définitions.

En effet, l'institution policière étant en charge du maintien de l'Ordre Public, il est utile de rappeler l'origine et la définition des mots « Police » et « Ordre Public » :

La police

Le premier sens du mot grec « Polis » est « ville » puis « règlement de la cité ». Il sera celui retenu jusqu'à la fin de l'Ancien Régime.

Puis l'institution policière, en charge de l'administration de la cité puis de la ville, est devenue l'enfant des temps modernes, de la croissance démocratique des états et des exigences de sécurité.
Cette évolution est résumée dans cette citation de Bertrand de JOUVENEL :

« ***la puissance policière a grandi à l'ombre de la démocratie*** ».

En ce début de XXI° siècle, la définition retenue regroupe deux phénomènes :

• Ensemble des règles imposées aux membres d'une collectivité organisée afin d'assurer l'Ordre Public et permettre à ses membres d'exercer leurs libertés et droits.
• Corps de fonctionnaires chargés de faire appliquer ces règles indispensables à la vie en société.

Il apparaît donc rapidement évident et inévitable une constante opposition entre les prérogatives qu'exercent les détenteurs du pouvoir et la liberté et les droits des individus :

La police est l'organisme chargée à la fois de faire appliquer les règles nécessaires à un certain Ordre Public et à la paix sociale, et de garantir l'exercice des libertés des individus.

L'ordre public

Il s'agit d'une notion juridique qui englobe l'ensemble des règles nécessaires au bon fonctionnement de l'État. Ce concept affirme la suprématie de l'intérêt général sur les intérêts particuliers, qui ne peuvent, même par convention, aller contre lui.

Plus spécifiquement, en droit administratif, l'Ordre Public correspond à un ensemble de conditions qui, à un moment donné, sont jugées nécessaires au déroulement de la vie normale de la société.

En effet, l'État, la société, la collectivité sont mis à mal lorsque ces règles ne sont pas respectées par les membres qui la constituent et qui, pourtant, en ont besoin, ou n'acceptent qu'une partie du contrat.

Le non respect de ces règles constitue des infractions dont l'ensemble est classé sous le terme générique de « criminalité » ou « délinquance » selon le niveau de gravité de l'atteinte portée à l'État, à la société, à la collectivité ou aux personnes.

L'Ordre Public, que la Police a pour mission de maintenir, peut faire l'objet de menaces et d'attaques de la part des membres même de la collectivité auxquels ils appartiennent.

Ces menaces revêtent plusieurs formes :

Les atteintes aux personnes :
- violences physiques (mort, viols, enlèvements, coups et blessures volontaires ou involontaires…)
- violences morales (harcèlement, menaces….),

Les atteintes aux biens dont les plus caractéristiques et les plus fréquentes sont les vols avec ou sans effraction, avec ou sans violence sur les personnes, les incendies, les dégradations sous toutes les formes, le racket …),

Les atteintes à la sûreté de l'État qui ont pour objectif de mettre en péril :
- les grands principes démocratiques par la commission d'attentats, d'homicides, d'enlèvements, d'agressions violentes...,

- les institutions gouvernementales, politiques, territoriales, et administratives par la commission d'attentats, de meurtres, d'actes de corruption ...,
- l'économie nationale par la commission d'actes de sabotage, d'abus de biens sociaux, de prise illégale d'intérêt, d'escroqueries, de faits d'espionnage économique…

Tous ces actes, regroupés sous le terme générique de « criminalité », sont le fait d'acteurs qui recherchent un intérêt idéologique, politique, économique, financier, personnel ou collectif :

- les organisations criminelles quelque soit leur importance, leur localisation, leur niveau, mais dont la principale motivation est le profit lucratif personnel,
- les associations de malfaiteurs terroristes nationales, internationales, d'État…, dont la raison d'être est d'imposer des règles autoritaires, révolutionnaires, objectifs pour lesquels elles doivent commanditer ou commettre des actes criminels leur permettant de financer leurs activités et imposer leurs vues. De ce fait elles satisfont également un intérêt personnel.

Face à ces attaques, des ripostes législatives et réglementaires, donc légales et démocratiques, sont mises en place par les États :

- le code pénal qui définit les infractions punissables, leurs éléments constitutifs, légal, moral et matériel, et les sanctions applicables,
- le code de procédure pénale qui affirme les règles d'organisation et de fonctionnement des institutions créées pour identifier les auteurs des faits, déterminer leurs responsabilités, qualifier ces actes de contraventionnels, délictuels ou criminels et prononcer des sanctions adaptées prévues par la loi.

- les législations et réglementations fiscales, économiques, du travail, de sécurité publique,

- les institutions policières, judiciaires, administratives …

- les techniques opérationnelles policières, judiciaires, administratives,

- les besoins opérationnels techniques, scientifiques, législatifs de la police et des services concourant à la sécurité intérieure et extérieure.

Mais, afin de déterminer la qualité et la quantité des ripostes à mettre en œuvre, il est important de connaître les méthodes illégales de ces malfaiteurs :

- Détournement à leur profit des mesures sociales, financières et économiques définies par les institutions, pour le bien-être des citoyens,
- Utilisation pour exercer leurs activités illégales des dispositions techniques, législatives et réglementaires mises à la disposition de l'ensemble des citoyens par les autorités,
- Appropriation à leur seul profit criminel des progrès économiques, scientifiques et techniques résultant de l'évolution de la société,

- Revendication, en cas d'arrestation, des grands principes de la DEMOCRATIE qu'ils ont pourtant volontairement bafoués.

En effet, toutes ces dispositions démocratiques sont utilisées, non pas pour l'évolution positive de la société, mais pour le profit personnel des dirigeants des organisations criminelles, des associations de malfaiteurs terroriste, donc des prédateurs de la société.

Il apparaît donc évident que :

- les agresseurs de la société ont à leur disposition les protections et moyens que celle-ci a mis en place pour protéger ses membres. Et c'est bien là, le nœud du problème : ***la société doit combattre un adversaire qui bénéficie des mêmes moyens qu'elle mais qu'il peut mettre en œuvre sans respecter aucune règle, ni aucune retenue.***

- ces mêmes prédateurs utilisent les progrès scientifiques et technologiques, mises à la disposition des membres de la société pour leur bien-être, qui leur permettent de se procurer de nouveaux et nombreux profits illégaux et d'optimiser leurs activités criminelles au préjudice de la société.

Le défi le plus important pour la Société, afin de défendre ses membres et ses principes d'organisation et de fonctionnement, est de définir et de mettre en œuvre des réponses tout en respectant les grands principes démocratiques que ses adversaires utilisent tout en les détournant et les invoquant pour leur propre protection dans leurs activités criminelles. Ce sont :

- des pratiques d'autodéfense contrôlées et contrôlables : textes de loi, des règlements, des obligations, des contrôles…

- la mise en place d'obstacles légitimes : obligations et formalités à respecter…

- des techniques professionnelles propres aux institutions policières, judiciaires et administratives réglementées et encadrées.

Pour assurer le défense de la société, il est impératif de définir une stratégie de défense reposant sur la prévention et la répression et des méthodes d'investigations pouvant, elles même, porter atteinte, mais sous contrôle démocratique, aux droits et libertés des citoyens, qu'elles sont censées défendre :

- Identification des menaces
- Identification des auteurs de ces menaces
- Réunion des éléments de preuve
- Localisation des auteurs
- Interpellation des auteurs avant, si possible, la commission des méfaits
- Mise à disposition de la Justice de ces malfaiteurs

Cette stratégie, pour être efficace, a besoin de :

- moyens techniques et scientifiques,
- bases de données d'information,
- dispositions législatives et réglementaires,
- moyens de contrôle,
- la confiance des autorités et des citoyens,
- des garanties de formation, de probité, de sanction.

Il apparaît donc que les défenseurs de l'Ordre Public ont l'image de marque qu'ils méritent, mais la société a les représentants de l'ordre qu'elle mérite, en fonction des moyens qu'elle accepte de mettre à leur disposition.

Mais il existe un dilemme à résoudre : les citoyens ont besoin de l'Ordre Public pour vivre libres, mais de marges de manœuvre pour satisfaire leurs besoins individuels pas toujours compatibles avec ceux de la société à laquelle ils appartiennent et sur laquelle ils comptent.

En résumé, les citoyens doivent accepter, pour pouvoir exercer leurs droits, d'avoir des devoirs et des obligations parfois contradictoires.

La loi « Informatique et Libertés » fait partie de ces dispositions indispensables, mais elle doit être complétée et appliquée selon des réflexions les plus objectives possibles. Ces réflexions doivent être politiques, au sens étymologique du terme.

En conclusion, il est indispensable, pour mener ces réflexions, d'avoir toujours en tête cette citation de Paul VALERY : « Si l'État est fort, il nous écrase, si l'État est faible, nous périssons ».
Les techniques informatiques, pour permettre aux citoyens de bénéficier de libertés dans les meilleures conditions de sécurité, doivent leur imposer des servitudes.

La réponse à la question posée n'est pas une alternative mais un cumul indispensable, **Informatique : Servitudes pour garantir les Libertés**.

M. François GIQUEL

Conseiller maître à la Cour des Comptes, vice-Président de la CNIL

Au sens strict, le terme d'ordre public ne figure pas dans le texte de la loi de 1978. D'ailleurs, dans sa globalité, l'ordre public ne relève évidemment pas de la compétence de la CNIL. En revanche, l'article 26 fait un sort particulier aux traitements de données à caractère personnel « *qui intéressent la sûreté de l'État, la défense ou la sécurité publique, ou qui ont pour objet la prévention, la recherche, la constatation ou la poursuite des infractions pénales (…)* ». Cela circonscrit assez bien le champ de notre débat de ce matin.

J'essayerai de vous montrer, à propos de ces fichiers de police et de sécurité, d'abord l'importance de la loi de 1978 et le rôle joué par la CNIL au cours des vingt-cinq

premières années de son existence, puis les problèmes nouveaux que pose les évolutions les plus récentes, avant d'évoquer devant vous en dernier lieu quelques propositions de réponses concrètes.

1ère Partie : La loi du 6 janvier 1978 et l'action de la CNIL pour sa mise en œuvre ont permis de donner aux fichiers de police et de sécurité un cadre légal plus protecteur des données à caractère personnel, et donc de la vie privée et des libertés individuelles, que jamais auparavant.

Comme chacun le sait, les fichiers de police ont toujours existé, même avec des fiches manuelles et des boites à chaussures… Car pour faire son travail, la police a besoin d'informations. Mais ce n'est pas l'information, en soi, qui fait question, ce sont les modalités d'organisation, de conservation et d'utilisation de l'information qui peuvent accroître considérablement l'efficacité des fichiers, grâce notamment aux progrès exponentiels de l'informatique, et qui, posant des problèmes nouveaux au regard des libertés individuelles, rendent indispensable la reconnaissance de nouvelles garanties.

Or le code de procédure pénale, qui détermine notamment les règles de procédure garantissant les droits des personnes face à l'action policière ou judiciaire, n'évoquait pas les fichiers de police et ne comportent d'ailleurs toujours pas de dispositions générales relatives à l'ensemble de ces fichiers. C'est la loi du 6 janvier 1978 relative « à l'informatique, aux fichiers et aux libertés » qui a donné aux fichiers de police le premier encadrement juridique. La loi ne distinguant pas selon la nature des fichiers, l'ensemble des principes qu'elle édicte s'applique aux fichiers de police comme à tous les autres, moyennant quelques aménagements spécifiques pour certains d'entre eux.

Il en est résulté trois conséquences qui sont autant de garanties pour les citoyens.

La première garantie est qu'aucun fichier de police ne peut être mis en œuvre sans avoir été examiné par une autorité administrative indépendante, la première créée en France, et donc extérieure à l'institution policière : c'est le rôle central attribué à la CNIL, qui se prononce au vu d'un dosser de demande d'avis comportant un certain nombre d'informations obligatoires. **La deuxième garantie** est que tout fichier doit être créé par un texte réglementaire publié (sauf exception motivée) : c'est un grand principe de transparence. **La troisième garantie** est celle du droit d'accès : s'agissant des traitements qui intéressent la sûreté de l'État, la défense et la sécurité publique, le droit d'accès des personnes intéressées n'est certes pas direct, mais s'exerce par l'intermédiaire d'un membre de la CNIL, magistrat ou ancien magistrat qui procède à toutes les vérifications. La CNIL a ainsi reçu depuis sa création plus de 10 000 demandes (dont près de 2000 en 2004) et a procédé à plus de 17 000 investigations. Á cela s'ajoute le fait que la CNIL dispose d'un droit de contrôle d'office et permanent de tout fichier existant.

Tout cela signifie qu'aucun responsable de fichier n'est seul juge de l'opportunité de ficher quelqu'un, du choix des informations qu'il enregistre et de la durée pendant laquelle ces informations sont conservées.

Incontestablement, la loi de 1978 a donc très largement concouru à « faire sortir de l'ombre » les fichiers utilisés quotidiennement par la police dans l'exercice de ses missions et a conduit la CNIL, saisie par le gouvernement de demandes d'avis ou d'autorisations au fur et à mesure de la naissance (ou de la reconnaissance) de ces fichiers, à préciser sa position, certains diront sa doctrine, quant aux garanties devant entourer la création et l'utilisation des fichiers de police.

On pourrait en donner de nombreux exemples, mais je me contenterai d'évoquer les fichiers des services des Renseignements généraux et ceux de la police judiciaire.

Les fichiers des Renseignements généraux avaient eux aussi, bien entendu, toujours existé, du moins depuis que le service ou ses équivalents existaient, mais deux décrets du 14 octobre 1991 leur ont donné un fondement réglementaire plus respectueux des droits de chacun sur ses données personnelles. Sans revenir sur les longues et parfois difficiles discussions entre la CNIL et le ministère de l'intérieur, nous pouvons affirmer qu'un progrès considérable a été fait, en particulier en matière de transparence : ainsi la DCRG s'est engagée à rendre compte chaque année à la CNIL de ses activités de vérification, de mise à jour et d'apurement de ses fichiers et dossiers et à procéder à un examen tous les cinq ans du bien fondé et de la justification des informations détenues dans ses fichiers « *selon une procédure contrôlée par la CNIL* » ; surtout, dans le cadre du droit d'accès indirect, tout citoyen peut obtenir communication directe dans les locaux de la CNIL ou en Préfecture des informations figurant dans ces fichiers, dès lors qu'elles ne mettent pas en cause la sûreté de l'État, la défense ou la sécurité publique. Dans la pratique, c'est le cas aujourd'hui dans plus de 9 dossiers sur 10.

Pour le fichier national de police judiciaire recensant les informations recueillies par les services de police concernant les crimes, délits et certaines contraventions, et destiné à faciliter la recherche des auteurs d'infractions, dénommé Système de Traitement des Infractions Constatées (**STIC**), les discussions entre le ministère de l'intérieur et la CNIL ont été plus longues, puisque le premier projet a été présenté à la Commission en juin1994 et que le décret portant création du traitement a été publié le 5 juillet 2001. La CNIL a fait prévaloir les garanties qui lui semblaient devoir nécessairement entourer l'utilisation de ce fichier (une définition précise des personnes mises en cause, une durée de conservation des données tenant compte de l'âge de la personne et de la gravité de l'infraction, une mise à jour rigoureuse en cas de relaxe, acquittement, non-lieu ou classement sans suite, etc.). Mais surtout elle s'est opposée à ce que le STIC, fichier de police judiciaire, puisse être utilisé à des fins administratives, par exemple lors d'enquêtes de moralité.
De nombreux autres fichiers de police ont été créés avec l'avis favorable de la CNIL, sans poser de problèmes particuliers, tels que le FAED (avec droit d'accès direct des personnes concernées), le FPR ou le FVV.

Tout cela constitue un acquis important qu'il ne faut ni mésestimer ni oublier, c'est un socle sur lequel on doit continuer de s'appuyer. La loi du 6 janvier 1978 et ses principes sont peu à peu entrés dans les esprits et dans les mœurs ; la CNIL a élaboré au cas par cas, progressivement et avec la souplesse nécessaire, un certain nombre de

garanties concrètes, d'exigences de transparence, et a pu en faire prendre conscience à ses interlocuteurs dans les ministères concernés, non par des vétos ou des diktats, mais par le dialogue et un effort persévérant d'explication. De ce point de vue, les modifications apportées en août 2004 à la loi fondatrice ne devraient rien y changer, même si la CNIL, en vertu du nouvel article 26, ne dispose désormais que d'un pouvoir d'avis, il est vrai publié en même temps que le texte réglementaire.

2ème Partie : Aujourd'hui, nous sommes face à une situation nouvelle, où la loi intervient pour créer de nouveaux fichiers de police et de sécurité et régir leur fonctionnement.

Il suffira de prendre quelques exemples.

- **le FNAEG** : Le premier fichier national d'empreintes génétiques a été créé par une loi du 17 juin 1998 relative à la prévention et à la répression des infractions sexuelles ainsi qu'à la protection des mineurs. Il ne concernait que les crimes à caractère sexuel et seulement les personnes définitivement condamnées. Successivement, par la loi sur la sécurité quotidienne du 15 novembre 2001 et celle sur la sécurité intérieure du 18 mars 2003, une extension du fichier est intervenue dans trois directions : - la liste des infractions pénales a été élargie aux infractions non sexuelles, d'abord aux crimes puis à certains délits, - non seulement les personnes condamnées sont concernées mais aussi les personnes à l'encontre desquelles il existe des indices graves ou concordants rendant plausible qu'elles aient commis l'une des infractions pouvant donner lieu à enregistrement, - cet enregistrement est désormais possible sur décision d'un officier de police judiciaire agissant d'office.

Dans son avis sur le projet de loi de 2003, la CNIL avait considéré que cette extension modifiait profondément la nature même du fichier et impliquait en conséquence l'adoption de garanties nouvelles s'agissant tout particulièrement de ses modalités d'alimentation comme des règles de conservation et d'effacement des informations personnelles traitées.

- **le STIC** : Ici encore, c'est finalement par la loi que les principes de fonctionnement de ce fichier, ainsi d'ailleurs que son équivalent pour la gendarmerie nationale, JUDEX, ont été déterminés, des modifications substantielles étant à cette occasion apportées au STIC, en particulier sur le point majeur qui avait fait l'objet de discussions entre 1998 et 2001, l'accès à ce fichier de police judiciaire pour des fins administratives. D'abord par la loi sur la sécurité quotidienne de novembre 2001 puis par la loi sur la sécurité intérieure de mars 2003, l'accès au STIC a été autorisé pour un certain nombre d'enquêtes administratives préalables au recrutement de divers emplois publics et à l'habilitation ou à l'agrément des agents employés par les services privés de sécurité, ainsi que pour la délivrance ou le renouvellement des titres de séjour, l'instruction des demandes d'acquisition de la nationalité française, les décorations.

La CNIL a fait valoir en vain qu'il s'agissait d'un détournement de la finalité première de ce fichier conçu pour faciliter les investigations policières et la recherche des auteurs d'infractions et non pour servir de casier judiciaire parallèle.

Cependant, le Conseil Constitutionnel, a considéré que l'ensemble des garanties que donne la loi en matière de création et d'utilisation des fichiers de police « *est de nature à assurer, entre le respect de la vie privée et la sauvegarde de l'ordre public, une conciliation qui n'est pas manifestement déséquilibrée* ».

- Le FIJAIS : ce fichier, créé par la loi du 9 mars 2004 portant adaptation de la justice aux évolutions de la criminalité, est destiné à prévenir la récidive des auteurs d'infractions sexuelles déjà condamnés et à faciliter leur identification et leur localisation. Ainsi, les personnes inscrites dans le FIJAIS ont l'obligation de justifier de leur adresse une fois par an et de déclarer leurs changements d'adresse dans les quinze jours.

La CNIL n'a pas été consultée sur ces dispositions législatives, qui ont été introduites par amendement ; toutefois, ses modalités d'application ont été fixées par un décret du 30 mai 2005 pris après avis de la Commission (dans sa délibération du 10 mars 2005, la CNIL a été particulièrement attentive aux garanties de confidentialité devant entourer les conditions de fonctionnement et d'accès de ce fichier).

- les fichiers SALVAC et ANACRIM : la loi sur le traitement de la récidive des infractions pénales qui vient d'être votée par les deux assemblées comporte, à la faveur d'un amendement déposé par le gouvernement, la création (en fait une légalisation) de nouveaux fichiers de police judiciaire visant cette fois les « crimes présentant un caractère sériel », par l'ajout d'un article 21-1 à la loi sur la sécurité intérieure, alors que l'article 21 de cette loi donne déjà un encadrement précis aux fichiers de police judiciaire.

La CNIL a fait un certain nombre d'observations sur ce texte, qui n'est pas encore définitivement adopté.

- Enfin **le projet de loi sur la lutte contre le terrorisme** qui vient d'être déposé sur le bureau de l'Assemblée nationale comporte la création ou l'extension de divers fichiers et l'élargissement des possibilités de consultation des fichiers existants en dehors des missions de police judiciaire.

Il prévoit la mise en œuvre, au bénéfice des services de police et de gendarmerie spécialement chargés des missions de prévention et de lutte contre le terrorisme, d'un ensemble de dispositifs qui visent à :

- développer la vidéosurveillance des personnes sur les lieux publics,
- contrôler les déplacements des personnes susceptibles de participer à une action terroriste, tant sur le territoire national (lecture des plaques d'immatriculation des véhicules et photographie des passagers) que lors du passage des frontières de l'Union européenne (accès aux données de réservation et d'embarquement des compagnies de transport aérien, ferroviaire et maritime),
- contrôler leurs échanges téléphoniques et électroniques (accès aux données de connexion ou d'abonnement des opérateurs et prestataires de télécommunications),

- accéder à un certain nombre de fichiers centraux de police administrative du ministère de l'intérieur pour permettre l'identification des personnes et des véhicules.

Ces dispositifs s'appuient sur le principe de la mise à disposition des services de police et de gendarmerie, de façon permanente et en vue d'une exploitation systématique, de fichiers et d'enregistrements d'images susceptibles de concerner la totalité de la population et appelés à conserver des traces visuelles ou informatiques des actes de la vie quotidienne, des habitudes de vie et de comportements (le lieu où l'on se trouve à tel moment, l'heure d'une connexion, le lieu d'où l'on passe un appel à partir d'un mobile, le passage à tel péage d'autoroute, la destination d'un voyage, etc.). Á ce titre, seraient ainsi créés de nouveaux fichiers d'un dimension considérable et l'accès à des gisements de données existants, publics ou privés, serait largement ouvert.

Toutes ces mesures visent à accroître les moyens d'action et donc l'efficacité des services de police et de gendarmerie afin de garantir la sécurité de l'État et des citoyens et de lutter contre le terrorisme. Même si la France s'est dotée dès 1986, puis au cours des années suivantes, d'un ensemble de dispositions concernant la lutte contre le terrorisme, il est clair que les attentats de New-York, puis de Madrid et de Londres ont renforcé cette nécessité. Personne ne le conteste.

3ème Partie : Dans ce contexte nouveau, quelle doit être la position de la CNIL ?

- **1ère remarque** : toutes les mesures nouvelles qui viennent d'être évoquées résultent de dispositions législatives. S'il est vrai que, conformément à la loi de 1978-2004 (article 11), la CNIL est consultée par le gouvernement sur tout projet de loi relatif à la protection des personnes à l'égard des traitements automatisés et que les rapporteurs des deux assemblées ont toujours le souci d'entendre des représentants de la Commission avant le débat parlementaire, c'est le Parlement qui fait la loi, et c'est bien ainsi, évidemment. Il est vrai aussi que la loi renvoie à des décrets d'application les modalités de mise en œuvre de tel ou tel fichier : la CNIL est donc à nouveau saisie pour avis, avec un dossier précis à l'appui, ce qui lui permet de faire entendre ses préoccupations. Mais il arrive que le législateur laisse peu de latitude au pouvoir réglementaire et fixe lui-même tel ou tel point important ayant des conséquences sur la protection des données personnelles, par exemple la durée de conservation des données ou les catégories de personnes ou services pouvant y avoir accès.

- **2ème remarque** : l'analyse de ces dispositions législatives et réglementaires, toujours bien entendu dans le domaine qui est le nôtre, fait apparaître que sont souvent visés en même temps des objectifs de sécurité « classique » (sécurité quotidienne, sécurité intérieure, lutte contre la délinquance, lutte contre la criminalité organisée, etc.) et des objectifs de lutte contre le terrorisme, la lutte contre l'immigration clandestine ou illégale venant souvent s'y ajouter.

Or les actions liées aux objectifs de la sécurité classique, disons la lutte contre la délinquance, y compris dans ce que cela comporte de prévention et de lutte contre la

récidive, relèvent des services de police judiciaire, et d'ailleurs les grands fichiers que nous avons cités sont placés, comme la CNIL l'avait souhaité, sous le contrôle du Parquet : c'est le cas du STIC, du FNAEG, du FIJAIS, ces deux derniers étant d'ailleurs régis par des dispositions du Code de procédure pénale, tandis que la CNIL elle-même conserve tous ses pouvoirs de contrôle. Á priori, rien ne justifier ait une remise en cause des grands principes sur lesquels repose jusqu'à présent la protection des données personnelles : exigence d'une finalité légitime, déterminée et explicite du fichier ou du traitement, proportionnalité des moyens mis en œuvre, c'est-à-dire caractère adéquat, pertinent et non excessif des données collectées, durée de conservation adaptée, droit d'accès organisé, qu'il soit direct ou indirect, etc.

En revanche, les objectifs de lutte contre le terrorisme posent des problèmes plus complexes :

- d'une part, parce que la finalité de « prévention et de lutte contre le terrorisme » vient souvent s'ajouter à d'autres finalités préexistantes, notamment de police judiciaire, donnant ainsi des possibilités de consultation des données personnelles à de nouveaux services dans le cadre de missions moins strictement définies,

- d'autre part, parce que dans la lutte contre le terrorisme, la prévention constitue à l'évidence une dimension fondamentale de l'action. Or les outils techniques, administratifs, ou juridiques de la prévention relèvent de ce que l'on appelle « la police administrative », et se situent en amont des procédures de la police judiciaire, et donc du contrôle des autorités judiciaires,

- enfin, parce que la prévention est une notion extrêmement large et, par construction même, extrêmement imprécise, ce qui, une fois posée cette finalité, pourrait justifier l'emploi de toutes sortes de moyens, même les plus attentatoires aux libertés individuelles.

Face à cette problématique nouvelle, il faut rechercher des solutions qui, sans nuire à l'efficacité de l'action des services concernés, garante de la sécurité de tous, assurent au mieux la protection des données personnelles et des libertés à laquelle nos concitoyens sont également attachés. C'est ce qui a guidé la CNIL dans l'élaboration de son avis sur le projet de loi anti-terrorisme, qui insiste notamment sur les points suivants :

1- Face à des circonstances exceptionnelles, comme celles que crée la menace terroriste actuelle, les nouveaux dispositifs juridiques et techniques envisagés devraient être considérés eux-mêmes comme exceptionnels, et donc limités dans le temps.
2- Au terme de cette première période, comme au terme de chacune des prorogations éventuelles, chacun des dispositifs devrait faire l'objet d'un rapport d'évaluation.
3- En tout état de cause, la finalité de chaque dispositif ou traitement devrait être aussi déterminée et explicite que possible.

4- Les services habilités dans le cadre de la lutte contre le terrorisme à utiliser les dispositifs informatiques ou à consulter les fichiers devraient être précisément et limitativement désignés.
5- Une information claire et transparente de l'ensemble des citoyens sur les nouveaux dispositifs mis en œuvre et les nouveaux droits de consultation accordés devrait être faite de façon claire et permanente , par tous moyens appropriés.

J'ajouterais volontiers, à titre personnel, que, si l'on décide, pour des raisons touchant à la sûreté de l'État et à la sécurité publique, de mettre en œuvre, même pour un temps limité, un dispositif exorbitant du droit commun de la protection des données personnelles, il conviendrait de prévoir sous des formes à déterminer une intervention d'un organe indépendant extérieur au service concerné avant tout accès à certains fichiers, comme le fait par exemple le projet de loi anti-terrorisme pour l'accès de certains services aux données de connexion.

C'est pourquoi nous devons être tous vigilants, dans un contexte où la menace terroriste est réelle, sérieuse et grave et la demande de sécurité de nos concitoyens, extrêmement forte, mais où la démocratie doit continuer d'affirmer les valeurs de liberté qui la fondent. La CNIL assume pour sa part cette mission de vigilance que, dans le domaine de la protection des données personnelles, le législateur de 1978 lui a confiée, et celui de 2004 renouvelée, même si ce n'est pas toujours facile. Elle le fait et continuera de le faire en s'appuyant sur quelques principes simples et de bon sens, qui sont ceux de la convention 108 du Conseil de l'Europe comme de la directive européenne de 1995, et qui figurent aussi à l'article 6 de notre loi : que veut-on faire au juste ? les moyens sont-ils bien appropriés et proportionnés ? N'y a-t-il pas d'autres solutions plus respectueuses de nos libertés ?

4. La réponse de l'industrie

M. Jean-Claude NASSE
Délégué général de l'Association française des sociétés financières

M. Philippe NOGRIX
Sénateur de l'Ille-et-Villaine, membre de la CNIL en charge du secteur monnaie et crédit

Philippe NOGRIX
Sénateur de l'Ille-et-Villaine
Membre de la CNIL en charge du secteur monnaie et crédit

Il ne s'agit pas de répondre point par point mais de mettre en perspective la nouvelle loi au regard des impératifs des professionnels et je vous propose le canevas suivant :

Faire connaître la loi informatique et libertés demeure un objectif : ce constat peut sembler paradoxal plus de 25 ans après la loi mais le milieu des PME est loin d'avoir pris conscience de cette loi ce qui explique la volonté de prendre appui sur le réseau des Chambres de Commerce et d'Industrie (CCI) identifiées comme des relais potentiels auprès des entrepreneurs, ainsi que sur les organismes professionnels qui se font ainsi le relais des règles existantes et également en retour vers la CNIL des préoccupations de leurs adhérents.

La loi nouvelle reconnaît la place des professionnels : C'est la reconnaissance des règles professionnelles sur lesquelles la CNIL donne désormais un avis de conformité , elle l'a fait en 2005 pour 2 codes de déontologie concernant l'e mailing (sollicitations électroniques non sollicitées). La profession bancaire pourrait envisager cette démarche.

1. Un paradoxe à éclaircir : le renforcement du contrôle a priori pour le secteur privé alors que l'un des objectifs du législateur est d'alléger les formalités

Le régime d'autorisations constitue une novation majeure de la nouvelle loi qui renforce le niveau de protection offert aux personnes.
Par le passé, la CNIL avait regretté à de multiples reprises de ne pas avoir de pouvoir de blocage vis à vis des traitements du secteur privé.
Désormais elle dispose d'un pouvoir d'autorisation et entend en faire application pour les traitements les plus sensibles :

Le régime d'autorisation délivré par la CNIL pour certains traitements sensibles du fait de la finalité poursuivie (traitements d'exclusion..) ou de la nature des informations traitées (données biométriques, appréciations sur les difficultés sociales des personnes) constitue une novation importante de la loi «informatique et libertés». Désormais, le régime de formalités ne dépend plus seulement d'un critère organique, c'est à dire l'appartenance du responsable de traitement au secteur public ou au secteur privé, mais d'un critère matériel, à savoir le caractère sensible du traitement du fait des risques effectifs qu'il fait peser sur les personnes concernées par le fichage.

Après un an d'application de la nouvelle loi, il s'avère que la CNIL procède à une interprétation favorable aux droits des personnes, s'agissant des traitements automatisés susceptibles, du fait de leur nature, de leur portée ou de leurs finalités, d'exclure des personnes du bénéfice d'un droit, d'une prestation ou d'un contrat en l'absence de toute disposition législative ou réglementaire (article 25.I.4°). Pour autant soucieuse de ne pas créer de contraintes trop lourdes, elle utilise la faculté de simplification offerte par l'autorisation unique d'où les 2 projets d'autorisation unique pour le score et le blanchiment d'argent qui seraient des modèles non obligatoires pour les organismes voulant simplifier leurs formalités.

Le législateur a choisi une formulation reprenant les termes mêmes de la directive européenne du 24 octobre 1995.
La portée de cet article est d'emblée fort large du fait de la coexistence de différents éléments : il s'agit de traitements qui sont « susceptibles » d'exclure une personne et non pas seulement de ceux qui excluent avec certitude et sans discussion possible une personne. Le caractère systématique de l'exclusion n'est donc pas une condition nécessaire de l'application de ce critère ; les traitements en question sont ceux qui ont pour finalité l'exclusion mais aussi ceux qui, alors même que la finalité du traitement ne réside pas dans l'exclusion, ont pour nature ou pour portée d'exclure du bénéfice d'un droit, d'une prestation ou d'un contrat ;
le texte ne vise pas seulement l'exclusion du bénéfice d'un droit mais aussi l'exclusion d'une prestation ou d'un simple contrat, ce qui lui confère immédiatement une portée beaucoup plus large.

Exemples : sur la pertinence des critères et paramètres du score, la CNIL lors des refus d'autorisation auxquels elle a procédé, a demandé de justifier de la pertinence ce qui a conduit les établissements concernés à renoncer à certains critères.

2. Pour utiliser une métaphore sportive, comment marquer l'essai, ou transformer la contrainte légale en élément de confiance ?

2.1 Transformer une contrainte légale en élément de confiance : c'est le pari de certains déclarants qui s'appuient sur la CNIL pour avoir un « label ». Cette tendance se développe.
La loi imposant des obligations aux responsables de traitement, la CNIL est inévitablement perçue comme une contrainte et c'est normal.
Par contre, cette contrainte se décline en trois aspects sur lesquels il est possible de jouer :

- **La lourdeur administrative** que représente l'accomplissement des formalités (déclaration ou demande d'avis) est la première source de récrimination : problèmes de compréhension du questionnaire, délai d'instruction du dossier.

La réponse consiste à simplifier les formalités, exonération de déclaration, déclaration simplifiée ou unique, ce mouvement est engagé et ne nécessite pas ici d'être développé.

- **La mauvaise compréhension des enjeux** : cet aspect apparaît plus fondamental car au delà des formalités, la doctrine de la CNIL n'est pas toujours bien comprise. La fixation d'une durée de conservation est toujours par exemple l'occasion d'un échange avec le déclarant qui dans un premier temps ne mesure pas les incidences de la conservation et souhaite conserver « pour toujours » les données collectées. Il lui est alors expliqué le principe du « droit à l'oubli » et la recherche d'une durée pertinente et en adéquation avec la finalité se fait souvent de concert. Toutes les recommandations de la CNIL en la matière sont forcément les bienvenues.

- **Le risque de conflits d'intérêts** : lorsque les enjeux « Informatique et Libertés » sont compris et admis, encore faut-il qu'ils n'entrent pas en conflit avec d'autres intérêt, susceptibles de prendre le pas sur eux, tels les intérêts commerciaux des entreprises. Ainsi dans l'opération de coordination pilotée par la Cnil à la fin de l'année 2003 sur la mise en œuvre du décret sur l'annuaire universel, le souci de celle-ci était que les campagnes de communication et d'information lancées par les différents opérateurs à destination des abonnés à la téléphonie mobile, sur les conditions d'inscription dans l'annuaire universel soient lancées en même temps. Or, il a semblé un temps qu'Orange prendrait de l'avance sur ses concurrents afin de bénéficier d'un effet d'annonce mais elle y a finalement renoncé. De même, les petits « spammeurs » qui savent agir dans l'illégalité prennent cependant le risque d'aspirer les adresses électroniques sur Internet car l'opération est financièrement rentable. La riposte consiste alors à faire largement usage des pouvoirs de sanction de la CNIL afin de faire prendre conscience à tous et surtout aux « spammeurs » des risques encourus.

2.2 La CNIL tient compte des réalités de la vie économique

- **Elle est une force de propositions** : Il ne s'agit pas seulement de dire ce qui ne va pas, pose problème au regard de la loi, comme c'est traditionnellement le cas dans le cadre de l'instruction des dossiers (courriers de demandes de complément ou d'observations lors de la délivrance de récépissés). Une nouvelle génération de déclarants veulent savoir ce qu'ils doivent faire pour que leur traitement « soit dans les clous » et ont toujours plus ou moins une crainte sourde que la CNIL s'oppose au dispositif. Cette force de proposition se retrouve dans les exemples de mentions d'informations devant figurer dans les conventions de compte signées par les clients des établissements bancaires, à la suite de l'audit mené sur le respect des prescriptions de la loi du 1978 combinée à la charte MURCEF signée par les banquiers. Idem pour les conditions d'information des abonnés à la téléphonie mobiles pour l'inscription dans l'annuaire universel, l'inscription dans une liste de mauvais payeurs ou de « fraudeurs »…. Le travail accompli autour des codes de déontologie est de la même nature (code de déontologie mégabases ; SNCD ; FIGEC).

- Elle fait prendre conscience des risques : désormais pourvue d'un pouvoir de sanction, la Cnil entend renforcer la visibilité sur les sanctions encourues et leur effectivité (afin d'éviter le syndrome du « tigre de papier »).

- Tout en gardant son indépendance : cette force de proposition, cette implication de la CNIL qui conduit à prendre position ne met-elle pas la CNIL en porte à faux par rapport à son indépendance ? Celle-ci ne signifie t-elle pas s'en tenir à un rôle d'arbitre entre les intérêts en présence (intérêts commerciaux le plus souvent contre droits des personnes physique) ? Ce rôle d'arbitre n'est déjà pas facile car reposant sur des intérêts antagonistes contrairement aux autres autorités de régulation telles l'ART ou la CRE qui doivent assurer à tous les mêmes règles du jeu

concurrentiel et n'ont pas à réaliser cette recherche du point d'équilibre entre intérêts légitimes des professionnels (accroître leur clientèle, la fidéliser, lutter contre la fraude et mieux appréhender le risque) et ceux des personnes physique (droit à la tranquillité, pertinence de l'inscription dans un fichier et exercice aisé de ses droits d'opposition, de rectification…..).

S'engager en faisant des contre-propositions, ce qui suppose de privilégier une technologie, une réponse technique au détriment d'autres outils du marché ce qui sera mal perçu par ceux qui ne sont pas retenus ou encore s'associer avec d'autres acteurs fait évidemment surgir la délicate question de l'indépendance.

En conclusion, la CNIL a un intérêt évident à créer un environnement au sein duquel l'industrie peut se conformer à ses obligations . Mais l'industrie a son rôle à jouer dans la création de cet environnement. Sensibiliser davantage les personnes concernées et les responsables de traitement à leurs droits et obligations constitue le meilleur moyen d'assurer la mise en œuvre de la nouvelle législation.

B. QUELLE RÉGULATION D'UN CONTINENT À L'AUTRE ?

14h30-18h00 Présidence de M. D.CHAGNOLLAUD

1. L'approche européenne : la régulation par des autorités de protection, les normes européennes.

M. Peter HUSTINX
Contrôleur européen de la protection des données

M. Bertill COTTIER
Directeur de l'Institut Suisse de droit comparé

M. Peter HUSTINX
Contrôleur européen de la protection des données

Monsieur le Président,
Mesdames et Messieurs,

J'ai le plaisir et le privilège de pouvoir prendre la parole lors de ce colloque organisé par la CNIL, le Sénat et l'Université Paris II, dans un cadre magnifique. En ma qualité de Contrôleur européen de la protection des données, j'apprécie tout particulièrement de pouvoir m'exprimer sur l'approche européenne liée à la protection des données à caractère personnel; j'aimerais remercier mon ami et cher collègue, Monsieur Alex TÜRK, président de la CNIL, de m'avoir invité à participer à cette rencontre très intéressante et enrichissante.

Le programme de cette après-midi met fortement l'accent sur le rôle des autorités de protection des données. Ces autorités jouent en effet un rôle important au niveau de l'approche européenne. Il s'agit toutefois de faire remarquer que ce processus s'effectue uniquement dans un cadre régulateur qui comprend des lois nationales de large portée, couvrant généralement la plupart ou l'ensemble des secteurs de la société, et préparant à la mise en place d'une approche intégrée du sujet du colloque. La manière dont les autorités de protection des données remplissent leurs tâches dans ce contexte constitue un facteur décisif de la réussite du modèle européen; c'est ainsi que l'on a pu, par exemple, répondre avec flexibilité à des intérêts concurrents et aux nouveaux développements.

J'ai l'intention, aujourd'hui, de traiter principalement la manière dont cette approche européenne a vu le jour et de faire des observations sur certains de ses éléments essentiels. Dans ce cadre, j'aimerais examiner le rôle joué par les autorités de protection des données et la façon dont elles dialoguent - ou pourraient dialoguer - avec d'autres acteurs-clés dans ce domaine. J'essaierai, à la fin de mon intervention, de dégager certains jalons pour l'avenir.

Cadre européen

Les premières initiatives prises dans les années 1970 aux niveaux nationaux, en Allemagne, en Suède et en France, ont résulté de réflexions initiales relatives à l'impact des technologies de l'information sur le rôle des gouvernements dans les sociétés démocratiques et sur la position des individus dans ces sociétés. Les premières initiatives prises au niveau international ont eu lieu dans le cadre du Conseil de l'Europe et se sont concentrées sur le rôle des droits fondamentaux et la portée de l'article 8 de la Convention européenne des droits de l'homme.

Comme vous le savez certainement, l'article 8 de cette Convention fournit un droit au respect de la vie privée et établit les conditions dans lesquelles des restrictions à ce droit s'avèrent acceptables, c'est-à-dire des restrictions reposant uniquement sur une base légale, au besoin dans une société démocratique, et accompagnées de dispositifs de sécurité appropriés contre les possibilités d'abus. Ces conditions ont été expliquées et définies dans le droit jurisprudentiel de la Cour européenne des droits de l'homme à Strasbourg.

Au début des années 1970, le Conseil de l'Europe a conclu que l'article 8 de la Convention des droits de l'homme comprenait un certain nombre de limitations à la lumière des nouveaux développements, tout particulièrement dans le domaine des technologies de l'information. Citons notamment la portée peu claire du concept de « vie privée », l'accent porté sur la protection contre les « autorités publiques » et l'insuffisance de la réponse apportée au besoin d'une approche positive et proactive, pouvant également concerner d'autres organisations et intérêts.

Ces réflexions ont résulté en l'adoption d'une Convention séparée sur la protection des données (1981), également connue sous le nom de Convention 108, qui a été ratifiée par 34 membres du Conseil de l'Europe, dont tous les pays faisant partie de l'Union européenne. Cette Convention considère la « protection des données » comme une protection des droits et libertés fondamentaux des individus, en particulier leur droit à une vie privée, relativement au traitement des données à caractère personnel les concernant. Cela montre que la « protection des données » va **au-delà** de la « protection de la vie privée »; en effet, elle touche également d'autres droits et libertés fondamentaux des individus, tout en s'avérant plus **spécifique** du fait qu'elle considère uniquement le traitement des données à caractère personnel. Cette Convention vise à protéger les individus contre la collecte, l'enregistrement, l'utilisation et la diffusion non justifiés des informations à caractère personnel.

La mise en œuvre de la Convention 108 dans les lois nationales a mis en évidence des différences dans les différents pays. En effet, il arrivait que les dispositions essentielles et les exigences de procédure donnant effet aux mêmes principes

s'avéraient très différentes. Ces différences ont menacé le développement du marché intérieur au sein de l'Union européenne, tout spécialement là où la fourniture des services publics et privés dépendait du traitement des données à caractère personnel et de l'utilisation étendue des technologies de l'information, que ce soit au niveau national ou au niveau transfrontalier.

Cela a incité la Commission européenne à présenter une initiative en vue d'harmoniser les lois de protection des données dans les différents États membres. Après quatre années de discussions, le processus a abouti à l'adoption de la Directive 95/46/CE. Les États membres sont, depuis lors, obligés d'adapter leur législation à cette directive et d'assurer, entre eux, le libre flux des données à caractère personnel. Cette directive a pris la Convention 108 comme point de départ, l'a précisée à de nombreux égards et a ajouté de nouveaux éléments. Parmi ces derniers, citons les tâches des autorités de contrôle indépendantes ainsi que la coopération entre ces autorités, de manière bilatérale et au sein d'un groupe de travail au niveau européen (groupe de travail article 29).

D'autres directives ont été adoptées depuis 1995, dans des domaines spécifiques. Un exemple type est constitué par la Directive 97/66/CE, remplacée par la Directive 2002/58/CE sur la vie privée et les communications électroniques. Cette dernière traite plusieurs sujets qui vont de la sécurité et la confidentialité des communications à l'enregistrement limité des données de trafic et de lieu et les communications indésirables telles que le « spamming ». La fourniture de services de base ou de services à valeur ajoutée utilisant différents types de réseaux est soumise à la directive générale et à la directive spécifique, ou plus exactement aux lois nationales qui mettent à exécution ces deux directives.

L'article 286 du Traité instituant la Communauté européenne, adopté en 1997 dans le cadre du Traité d'Amsterdam, stipule qu'il faut appliquer des règles similaires au niveau européen, dont la mise en place d'une autorité de contrôle indépendante. De telles règles ont été établies dans le Règlement 45/2001/CE du Parlement européen et du Conseil, qui est entré en vigueur en 2001. Ce règlement prévoit aussi la mise en place d'une autorité de contrôle indépendante, appelée « Contrôleur européen de la protection des données ». Cela constitue le cadre de mes activités axées sur les institutions et organes de l'Union européenne.

En mai 2003, la Cour européenne de Justice à Luxembourg a prononcé sa première décision relative à la directive 95/46/CE, dans le cadre d'une affaire autrichienne (« Rechnungshof »). La question consistait à savoir si les informations relatives aux salaires des fonctionnaires pouvaient être publiées afin de réduire le niveau des rémunérations. La décision prise par la Cour montre clairement que cette directive présente une portée étendue et qu'elle s'applique également au traitement des données à caractère personnel au sein du secteur public des États membres. La Cour s'est basée sur plusieurs critères tirés de l'article 8 de la Convention européenne des droits de l'homme pour évaluer la légalité de ce traitement. La décision montre également que toutes les parties concernées peuvent invoquer cette directive dans les tribunaux nationaux. L'on peut ainsi s'attendre à d'autres décisions de ce type dans un proche avenir.

Un autre point qu'il faut mentionner ici est l'accent porté sur la protection des droits fondamentaux dans le Traité constitutionnel, actuellement soumis à ratification dans les différents États membres (la France et les Pays-Bas l'ont rejeté, pour des raisons qui ne concernent pas la protection de ces droits). Le respect de la vie privée et familiale ainsi que la protection des données à caractère personnel sont traités comme des droits fondamentaux séparés dans les articles II-67 et II-68, ce qui constitue une reconnaissance du processus entamé au début des années 1970 au sein du Conseil de l'Europe. La protection des données est également mentionnée dans l'article I-51, sous le titre VI consacré à la vie démocratique de l'Union. L'on voit ainsi clairement que la protection des données est maintenant considérée comme un composant de base de « bonne gouvernance ». Il s'agit de mentionner que ce développement était aussi visible dans la Charte des droits fondamentaux adoptée en décembre 2000 à Nice, que personne n'a remise en question jusqu'à présent.

Finalement, il s'agit de préciser que la protection des données est de plus en plus souvent considérée, au niveau de l'Union européenne, comme une question « horizontale » dont la pertinence dépasse la prospérité du marché intérieur. Ce phénomène découle de la Constitution et se remarque aussi dans les décisions prises par la Cour. Il s'agit d'un développement opportun et bienvenu. Le programme politique de la Commission actuelle comprend plusieurs points où il sera possible d'obtenir de meilleurs résultats si l'on accorde, dès le début, de l'attention à la protection des données. Cela est également le cas pour le « troisième pilier » de l'Union européenne – la coopération dans le domaine de la sécurité, de la police et de la justice pénale – , ce qui se reflète par la présence de plusieurs propositions sur lesquelles je me penche actuellement en ma qualité de conseiller de la Commission, du Conseil et du Parlement.

Éléments essentiels

L'on remarque que l'approche européenne relative à la protection des données est étroitement liée à la protection des droits fondamentaux dans une « société de l'information » et au développement du droit à la « protection des données à caractère personnel » comme droit fondamental, clairement différencié du « droit à la vie privée ».

J'estime que cette distinction est très utile. Ces deux droits possèdent leurs propres caractéristiques qui contribuent à une meilleure protection des individus concernés. Il est intéressant de voir comment des éléments similaires tels que le besoin d'une base légale, un but légitime, la proportionnalité et des dispositifs de sécurité adéquats sont utilisés dans les deux cas: dans le dernier cas pour empêcher les ingérences excessives dans la vie privée et dans le premier cas pour garantir un traitement juste et légal des données à caractère personnel, peu importe si l'on se trouve ou non dans la portée du droit à la vie privée. La décision prise par la Cour européenne de Justice relativement au cas autrichien a illustré de manière intéressante comment cette approche peut fonctionner dans la pratique.

Les principaux éléments du droit à la protection des données ont été mentionnés dans l'article 8 de la Charte et dans l'article II-68 du Traité constitutionnel. Bien entendu, l'élément décisif est constitué par le fait que la protection est accordée aux « données à caractère personnel » en général. Ce concept a été défini dans la Directive 95/46/CE; toutefois, les opinions diffèrent sur la manière de l'appliquer dans la pratique. Le groupe de travail article 29 est sur le point d'entamer la réalisation d'une analyse commune qui devrait également clarifier la manière dont ce concept s'articule par rapport aux nouvelles technologies. Je me réjouis beaucoup de cette action et j'ai l'intention d'y apporter ma contribution.

Le deuxième élément principal est que les données à caractère personnel doivent être traitées loyalement, à des fins déterminées et sur la base du consentement fourni par la personne concernée ou une autre base légitime prévue par la loi. L'on retrouve ici, de manière résumée, les principes relatifs à la protection des données fixés dans la Directive 95/46/CE, qui mettent l'accent sur la nécessité de collecter des données uniquement pour une finalité spécifique et légitime et de limiter les autres traitements à des fins qui s'avèrent compatibles avec cette finalité initiale.

Pour ce qui est du besoin d'une base légale, la directive mentionne le « consentement » comme une option parmi six éléments – dont l'exécution d'un contrat et le respect d'une obligation légale; cependant il est clair que tous les « consentements » doivent être spécifiques, fondés sur la connaissance des faits et fournis librement. Il ne s'agit ainsi que d'une option nécessaire et suffisante dans un nombre limité de cas, inférieur à ce que l'on suppose souvent dans la pratique. La directive prévoit des règles plus strictes en cas de traitement de données sensibles.

Le besoin d'un « traitement loyal » implique la fourniture d'informations suffisantes aux personnes concernées par les données, même si leur consentement n'est pas requis. J'estime que cette exigence est souvent sous-estimée et insuffisamment respectée dans la pratique. En d'autres termes, il reste encore de nombreuses améliorations à apporter.

Le troisième élément principal est que chacun devrait avoir le droit d'accéder aux données qui le concernent et le droit d'obtenir une rectification si nécessaire. La directive prévoit ces droits en fournissant davantage de détails; elle accorde également le droit d'opposition, soit pour des motifs contraignants liés à la situation particulière ou sans restriction dans le cas du « marketing direct ». Ce « droit d'opposition » constitue un élément type du droit européen basé sur l'expérience française. Ces différents droits et la possibilité de fournir ou de refuser le consentement permettent aux individus concernés de connaître et d'influencer le traitement de leurs données à caractère personnel, du moins dans une certaine mesure.

Le dernier élément essentiel de l'approche européenne est que le respect de ces règles doit être soumis au contrôle d'une autorité indépendante. Ce point est expressément mentionné dans la Charte et le Traité constitutionnel. Un protocole additionnel à la Convention 108, entré en vigueur en juillet 2004, demande maintenant aux différentes parties de mettre en place des autorités de contrôle, qui doivent exercer

leurs fonctions de manière entièrement indépendante, ce qui constitue un élément essentiel d'une protection efficace des individus.

Rôle des autorités

Pour ce qui est du rôle des autorités de contrôle, différents modèles ont été utilisés pendant longtemps dans plusieurs États membres. L'approche initiale suédoise était basée sur la nécessité générale d'autorisation préalable. L'approche française était beaucoup plus sélective, alors que l'approche suivie en Allemagne prévoyait un contrôle sur une base « ex post » et des pouvoirs de réaliser des recommandations. La Directive 95/46/CE a harmonisé en grande partie les rôles et les pouvoirs des autorités de surveillance.

Une condition essentielle est que les autorités de contrôle doivent exercer leurs fonctions en toute indépendance. La question de savoir ce qu'il faut entendre par « indépendance » et ce que ce concept exige est traitée actuellement par la Commission européenne, suite à une plainte déposée par un citoyen allemand relativement à la position d'une autorité régionale. La décision qui sera prise présente un intérêt non seulement pour l'Allemagne, mais aussi pour les autres États membres.

La directive prévoit que les autorités de protection des données doivent être consultées relativement aux projets de règlements liés à la protection des données à caractère personnel. Le règlement sur lequel reposent mes activités prévoit l'obligation de me consulter lorsque la Commission adopte une proposition de législation qui a un impact sur la protection des données à caractère personnel. Il s'agit d'un instrument très important de contribution au processus législatif; j'ai publié cette année un document de politique générale sur la manière d'exercer ce rôle.

La directive fournit également aux autorités des pouvoirs d'investigation et d'intervention, ainsi que la capacité à engager des poursuites ou à communiquer les infractions aux autorités judiciaires. Dans un certain nombre d'États membres, ces pouvoirs permettent de faire des ordonnances et d'imposer des sanctions, qui ont force obligatoire s'il n'y a pas d'opposition à la décision. Dans tous les cas, il est nécessaire que les autorités de contrôle puissent exercer une réelle influence. Dans ce but, il me semble que ces autorités devraient aussi être en mesure de définir leurs priorités et de déterminer les affaires qui doivent recevoir le plus d'attention.

Un élément important de la directive est que les autorités sont obligées de coopérer entre elles dans la mesure qui s'avère nécessaire pour exécuter correctement leurs tâches. Dans la pratique, cela arrive de plus en plus souvent, de manière limitée pour des affaires qui présentent des dimensions internationales ou plus largement dans le cadre du groupe de travail article 29. Une coopération se met en place pour les affaires liées aux flux de données vers des « pays tiers » présentant un niveau inadéquat de protection. Le groupe de travail article 29 est également en train de préparer une opération commune relative à la mise en application, ce qui permettra d'améliorer l'efficacité de la coopération dans un contexte international.

Relations pertinentes

Si l'on examine maintenant la manière dont les autorités de contrôle dialoguent avec les organisations responsables du traitement des données à caractère personnel, l'on note certains développements intéressants.

Premièrement, il est évident que la directive a encouragé une approche plus sélective en matière de surveillance, permettant d'effectuer une distinction entre les cas pertinents sur la base des risques impliqués. Seuls les cas qui présentent une probabilité de risques spécifiques sont soumis à un contrôle préalable par l'autorité de contrôle, cela sans distinction du secteur concerné ; les lois nationales peuvent toutefois définir les systèmes considérés comme présentant des risques spécifiques.

D'autres systèmes sont sujets à une notification préalable à l'autorité de contrôle. La directive autorise cependant d'importantes exceptions à ce principe. La possibilité d'accorder des dérogations à certaines catégories qui ne présentent pas de risques, pourvu que certaines conditions soient remplies, est clairement basée sur l'expérience faite dans certains pays en matière de dérogations similaires (par exemple les « normes simplifiées » de la CNIL).

La deuxième option – qui prévoit la nomination d'un délégué (ou correspondant) interne à la protection des données – s'avère même encore plus intéressante. Cette option a maintenant aussi été adoptée en France. Au niveau européen, les institutions et organes communautaires ont l'obligation de disposer d'au moins un délégué à la protection des données, qui doit réaliser un certain nombre de tâches spécifiques. Ces personnes forment un réseau de grande valeur rassemblant des expériences de « première ligne » ; mon bureau collabore avec elles pratiquement chaque jour. J'ai l'intention, dans le courant de ce mois, de publier un document d'orientation sur le rôle de ces délégués.

D'une manière générale, la directive encourage également le développement de codes de conduite pour différents secteurs sociaux ou économiques. Ces différents instruments sont conçus pour encourager un développement dans lequel d'autres acteurs peuvent se charger d'une intégration efficace des règles et principes liés à la protection des données dans les pratiques normales des organisations concernées. Un autre point essentiel est que la protection des données constitue également un élément important de la qualité adéquate en cas de fourniture de services par voie électronique. La Constitution de l'Union européenne considère également ce point comme un élément de « bonne gouvernance ».

Pour ce qui est des relations avec les individus concernés par les données, le premier objectif des autorités de contrôle devrait être de les sensibiliser et de leur permettre d'exercer leurs droits. Les responsables du traitement pourront ainsi être progressivement encouragés à s'investir davantage dans leurs relations avec les individus concernés par les données. Se concentrer sur la sensibilisation des responsables et des individus concernés par les données constitue une bonne stratégie pour les autorités de contrôle.

Dans ma fonction précédente de président de la commission néerlandaise de protection des données, j'ai eu des expériences enrichissantes relativement à

l'implication d'organisations ayant une fonction d'intermédiaire, telles que les associations de consommateurs, les syndicats, etc. Ces derniers étaient très actifs dans le domaine de la protection des données au niveau de l'emploi. La loi néerlandaise leur donnait également la possibilité d'intenter des procès dans l'intérêt de leurs membres.

Pour les autorités de contrôle, cela implique un environnement plutôt complexe, composé de différents secteurs, aux besoins et exigences variés. Les autorités indépendantes ne peuvent pas – et, à mon avis, ne devraient pas – se retenir d'établir des relations avec les différents organismes et personnes concernés. Au contraire, beaucoup de mes collègues ont découvert la nécessité de collaborer avec des partenaires et des alliés pour exécuter leurs tâches; certains d'entre eux ont connu une grande réussite à cet égard. Le fait que la CNIL comprend des membres provenant d'horizons différents montre un développement du même type.

Remarques de conclusion

J'aimerais conclure en présentant deux brèves réflexions, qui ont toutes deux trait à l'efficacité de la protection des données et à la coopération internationale.

Il est important de mettre en évidence les valeurs et les principes sous-jacents de la protection des données, comme je l'ai fait aujourd'hui en présentant l'approche européenne. Toutefois, je suis d'avis que c'est « l'efficacité » qui constitue le principe le plus important de la protection des données. Les bons principes « théoriques » sont nécessaires mais les bons principes « actifs dans la pratique et en conformité avec celle-ci » sont encore meilleurs. Le rôle des autorités de contrôle consiste principalement à garantir ce type de conformité. Plus ces autorités enregistrent des résultats positifs dans l'exécution de cette tâche, plus leur objet s'en trouvera favorisé.

Les environnements différents peuvent exiger des solutions ou des combinaisons de solutions différentes. J'estime qu'il n'y a pas de recette unique pour parvenir à une bonne surveillance. Mais je pense que, dans ce domaine, nous pouvons apprendre les uns des autres. C'est la raison pour laquelle j'ai proposé, lors de la conférence internationale qui s'est déroulée récemment en Suisse, d'échanger nos expériences de manière plus structurée et systématique. Les principes de « bonne surveillance » peuvent constituer une solution pour le long terme et je me réjouis de la poursuite des discussions sur leur faisabilité. Dans tous les cas, il est important d'atteindre un certain degré d'harmonisation des stratégies et des méthodes de travail en considération de l'objectif de la Directive 95/46/CE visant à harmoniser la protection des données dans l'Union européenne.

2. Un régime unique de protection des données pour une pluralité des systèmes politiques, judiciaires, économiques et culturels : utopie ou réalité ?

M. Bertil COTTIER
Directeur de l'Institut suisse de droit comparé

1. Introduction

Mesdames, Messieurs, je sais que le comité d'organisation va m'en vouloir profondément, **mais je me sens obligé de modifier**, d'emblée et unilatéralement, **le titre de mon exposé**. Rassurez-vous je n'ai pas décidé sur un coup de tête de vous parler de toute autre chose – tel le développement du tourisme à Montreux au XIXe siècle– non, je souhaite simplement changer une petite partie du titre. **Sa fin ne sera plus : *utopie ou réalité ?* Mais *une réalité à quel prix* ?**

En effet, la question s'avère finalement mal posée (cela dit j'avoue volontiers que j'ai participé à sa formulation et n'échappe donc pas à une part de responsabilité). Mais voilà je suis persuadé qu'un régime unique de protection des données n'est pas une quelconque rêverie de juriste en mal d'internationalisation. Avec l'augmentation considérable des échanges internationaux et la mobilité croissante des personnes, des biens, des services et des capitaux à l'échelon de la planète, plus aucun domaine du droit ne résiste aux efforts d'unification. Voici quelques années il était encore impensable d'envisager la simple harmonisation du droit de famille ou du droit des successions. Le printemps passé, la Commission européenne a brisé le tabou : dans un livre vert, elle propose très sérieusement de créer, je cite, « un instrument communautaire unique relatif aux successions et testaments »[1]. Percée aussi en droit de famille, avec un autre livre vert, également publié cette année, lequel prévoit l'unification des règles sur « le droit applicable et la compétence en matière de divorce »[2].

Certes, ces avancées ne sont que régionales; il n'en demeure pas moins que même des domaines du droit réputés jusqu'à peu absolument immune à l'internationalisation, car profondément ancrés dans des traditions sociales et culturelles, sont désormais dans le collimateur de l'unification. Qui peut le plus peut le moins : rien n'interdit de tabler sur un prochain régime commun de la protection des données ; ce d'autant que la convergence des ordres juridiques est actuellement forte dans deux domaines sous-jacents à la protection des données : les droits de l'homme et le droit du commerce international. Reste à savoir, et c'est là la question cruciale, quand on pourra parler de réalité.

Demain ? la réponse est clairement non: un bref coup d'œil sur la carte du monde révèle de grandes disparités de régime de protection de données entre pays qui

[1] *Livre vert sur les successions et testaments, publié par Clunet, 2005*
[2] *Livre vert sur le droit applicable et la compétence en matière divorce, publié par Clunet 2005.*

consacrent un haut niveau de protection, pays qui consacrent une protection partielle ou précaire et pays pour qui la protection des données est encore terra incognita (une centaine d'États, pour la plupart africains et asiatiques). Un régime commun de la protection des données est-il cependant concevable d'ici une année ? d'ici cinq ans ? d'ici dix ans ? La réponse dépend de deux facteurs-clefs :

- la nature des obstacles juridiques, économiques et politiques à surmonter et
- l'existence de facteurs d'intégration propres à surmonter ces obstacles.

2. J'en viens d'abord aux obstacles : **le premier** qui vient à l'esprit est incontestablement **la différence entre les systèmes juridiques** de par le monde.

2.1. Les comparatistes classiques[1] établissent une distinction fondamentale entre **quatre systèmes juridiques** :

- le système de droit romano-germanique, fondé sur la codification des normes (cette famille regroupe la plupart des pays du continent européen ainsi que l'Amérique latine),
- le système de droit anglo-saxon (aussi dit de *common law*) qui privilégie une approche jurisprudentielle (le juge crée ou plutôt *énonce* la règle juridique),
- les pays de droit religieux basés sur une révélation divine des règles juridiques,
- les pays de droit socialiste où le droit est un instrument subordonné à la réalisation des objectifs de changement en profondeur de la société prônés par la doctrine marxiste-léniniste.

Réductrice, artificielle, voire dépassée, cette classification n'est aujourd'hui plus exempte de critiques. Quoi qu'il en soit, pour des raisons de pure commodité, je fonderai mon exposé sur la division classique en quatre systèmes.

Cela dit, je me dois de rappeler la prémisse à notre réflexion : l'internationalisation croissante des rapports et des échanges de toute nature, entraîne un mouvement, apparemment irréversible, de convergence des droits[2]. Convergence visible, pour ne pas dire éclatante, par le biais de traités internationaux ; convergence aussi, plus discrète mais pas nécessairement moins efficace, par réception, plus ou moins spontanée, plus ou moins opportuniste, de solutions étrangères. Exemple fameux de ces nombreux copier/coller législatifs : l'importation quasiment d'un seul tenant du Code civil suisse par la Turquie en 1926 ; son dirigeant d'alors, Kamel ATATÜRK, souhaitait disposer rapidement d'une législation de droit privé moderne et surtout laïque. La réception se poursuit: au milieu des années huitante la Suisse a renforcé dans son code civil la protection de la personnalité (art. 28ss) ; la Turquie lui a

---

[1] Avec à leur tête, René David et son ouvrage d'antologie : Les grands systèmes de droit contemporains (11ème éd, Paris 2002)

[2] Pour un bilan récent de la convergence des droits en Europe, voir E. Örücü, Looking at convergence through the eyes of a comparative lawyer, Electronic Journal of Comparative Law, vo. 9.2, Juillet 2005

aussitôt emboîté le pas : en 1987, elle introduisait un art. 24nouveau destiné, sur le modèle suisse, à offrir aux particuliers un instrument de défense de la vie privée[1].

Si les divergences entre les systèmes juridiques vont s'estompant, on ne saurait oublier que le rapprochement ne touche à l'heure actuelle que le contenu du droit, les solutions matérielles proprement dites. Les différences structurelles demeurent cependant profondes, voire inconciliables. D'un système à l'autre la méthodologie varie, à commencer par la hiérarchie des sources du droit : ici le droit législatif prime, là c'est la coutume non écrite, ailleurs les livres sacrés ou encore la doctrine du parti unique ; autre dissemblance importante : pour les romano-germaniques, la distinction entre droit privé et droit public est décisive, pour les anglo-saxons, elle joue un rôle mineur. De même, les techniques législatives divergent : les pays de *common law,* fondés sur la casuistique et plus sensibles aux questions de procédure édictent des textes à haute densité normative, truffés de dispositions descriptives et circonstanciées ; le droit romano-germanique, comme le droit socialiste, opère par le biais de normes générales et abstraites ; il privilégie une légistique déductive, au contraire de la *common law* qui s'est construite par induction.

Mais au-delà des différences formelles, surgit un problème beaucoup plus difficile à résoudre : la différence de culture juridique, c'est-à-dire le rapport qu'a le citoyen ou la société d'un pays donné avec son ordre juridique. Prenons un exemple, si aux États-Unis, le procès est le moyen courant, pour ne pas dire banal, de résoudre les litiges, au Japon, c'est *l'ultima ratio* : le procès trouble l'harmonie de la société parce qu'il désignera un gagnant et un perdant.

Les différences de culture juridique sont un champ d'exploration relativement nouveau pour les comparatistes, qui en tant que juristes sont souvent mal à l'aise avec la dimension sociologique, voire psychologique de la réalité. S'il est difficile de mesurer les conséquences des différences de culture juridique sur l'application d'un régime commun, on s'accorde à dire qu'elles menacent sérieusement une mise en oeuvre uniforme. La problématique est d'autant plus délicate que les fractures culturelles peuvent traverser un seul et même système juridique. Les Hollandais et les Allemands appartiennent tous deux au système romano-germanique, mais les premiers ont une approche pragmatique du droit, les seconds une approche dogmatique.

2.2. Mais il est temps de revenir à **la protection des données**. On sait que les trois juridictions pionnières en la matière (la Suède, la France et le Land de Hesse) ressortissent à **la famille romano-germanique**. Leurs législations ont servi de creuset, tant matériel que formel, pour les textes qui suivront, qu'ils soient nationaux ou internationaux, à l'instar de l'instrument phare qu'est la directive européenne 95/46 sur la protection des données. Fondés sur une approche prescriptive et systématique du droit, articulés autour de règles de comportement de nature générale et abstraite, ces textes se coulent dans la plus pure tradition continentale et concrétisent une vision générale de la protection de la personnalité qui dans la plupart des cas préexistait soit dans la Constitution, soit dans le code civil, voire dans

[1] *F. Eern, Persönlichkeitschutz und immaterieller Schaden, rapport présenté aux journées turco-suisse 1989, Publications de l'Institut suisse de droit comparé, vol 17, p. 19ss.*

le code pénal. Reste à savoir si cette conception romano-germanique de la protection des données, aujourd'hui de mise, peut trouver sa place dans des systèmes de *common law*, de droit religieux ou de droit socialiste. Mais voyons cela de plus près.

2.3. La famille de common law d'abord ; là tout a démarré sous d'excellents auspices : on sait que la notion même de *privacy* est née dans un pays anglo-saxon, sous la plume de deux avocats américains dont un futur juge à la Cour suprême[1] ; cela dit si l'article innovateur qui a conceptualisé la *privacy* est aujourd'hui encore un must pour chacun d'entre nous, sa consécration normative n'a pas suivi. Á ce jour, la *common law* ne reconnaît, toujours et encore, que quatre actions (torts) de protection de la vie privée ; ciblés, ces quatre instruments recouvrent des hypothèses éloignées des exigences de la protection des données classique[2]. Cela dit, même si les assises de la protection de la vie privée sont plus précaires qu'en droit romano-germanique, rien ne s'oppose à l'essor de législations sur la protection des données sur le modèle continental : à témoin les récentes lois du Royaume-Uni et de l'Irlande; il est vrai que la directive européenne 95/46 leur a forcé la main.

D'autres pays anglo-saxons, notamment l'Australie, la Nouvelle-Zélande et le Canada ont aussi légiféré. Même si ces législations ne vont pas toujours aussi loin que le modèle européen, elles n'en sont pas moins très proches, à deux dissemblances majeurs près (je laisse de côté la technique législative). La première différence tient à la portée : le secteur privé jouit rarement d'un haut niveau de protection des données (j'y reviendrai plus détail lorsque j'évoquerai le cas des États-Unis). La seconde différence est une approche plus associative ou horizontale de la régulation : une grande place est faite à la soft law, notamment aux codes de conduite, lesquels sont même ici ou là promus au rang de sources primaires de la réglementation de certains domaines particuliers de la vie économique. C'est le fameux "co-regulatory model" si caractéristique de la culture administrative anglo-saxonne (un modèle qui, soit dit en passant, fait son chemin en Europe continentale : le récent code italien de la protection des données prévoit l'adoption de réglementations sectorielles d'entente entre les associations professionnelles et le « Garante per la protezione dei dati »).

2.4. Je passe maintenant à **la famille des pays de droit religieux**, et me concentrerai sur la plus grande d'entre-elles, les pays de droit musulman.

Il faut être conscient que dans ces pays toute législation est subordonnée à une exigence, plus ou moins forte selon les États, de conformité avec les canons de l'Islam, tel que définis par la source juridique suprême qu'est la Sharia (à savoir le Coran et les Hadiths, soit les commandements et exemples du Prophète). Á première vue on pourrait penser que ces prescriptions juridico-religieuses feraient peu de cas du quotidien des relations humaines ; il n'en est rien. Ainsi le Coran, contrairement à d'autres livres religieux, se soucie de la vie privée. D'abord plusieurs versets consacrent l'inviolabilité du domicile privé ; deux exemples :

---

[1] *S. Warren et L. Brandeis " The Right to Privacy", Harvard Law Review 1890, no 5.*

[2] *Intrusion upon seclusion, Publication of embarrassing private facts, Publicity placing a person in a false light et Appropriation of name, likeness and identity.*

> H-102/24:27. N'entrez dans des maisons autres que les vôtres que lorsque vous avez aperçu et salué leurs gens. Cela est meilleur pour vous.
>
> H-102/24:28. Si vous n'y trouvez personne, alors n'y entrez pas avant que permission vous soit donnée. Et si on vous dit: "Retournez", eh bien, retournez.

Ensuite, et encore plus intéressant, un verset fustige les *big brothers* de l'époque :

> H-106/49:12. Ô vous qui avez cru! (…) Ne vous espionnez pas. Ne médisez pas les uns en l'absence des autres.

Le droit musulman classique donc non seulement ne fait pas obstacle à la réception d'une protection moderne de la vie privée, mais encore en jette les bases. La Tunisie a montré la voie en adoptant une loi sur la protection des données en juillet 2004, calquée sur la directive européenne ; cette première n'est pas surprenante dans le mesure où ce pays maghrébin est l'un des plus ouvert sur l'Occident – son code de la famille accorde à la femme des prérogatives impensables dans le reste du monde arabe. Cela dit, le prochain pays musulman pourrait bien être, ô surprise, un État beaucoup plus pointilleux dans l'application à la lettre de la Sharia : le Pakistan ; le Parlement de ce pays doit se prononcer prochainement sur l'*Electronic data protection and safety act* de 2005.

2.5. Quelques mots sur les pays de droit socialiste : une catégorie aujourd'hui en voie de disparition. La famille des droits socialistes se caractérise par le primat absolu du politique sur le juridique, et dans son sillage, le primat de la collectivité sur l'individu. On comprendra dès lors que la protection de la personnalité, affirmation d'une douteuse autonomie personnelle, passe au second plan. Comme c'est le cas aujourd'hui encore dans le dernier grand pays d'obédience socialiste : la Chine. Pays qui, de plus, est encore tiraillé par la tradition confucéenne, guère plus favorable à la liberté individuelle. Confucius prônait en effet une société paternaliste et hiérarchique, centrée sur la subordination totale au chef de famille.

Malgré ce terreau doublement défavorable, les signes avant-coureur d'un renversement de paradigme sont là: le 27 juillet dernier un journaliste chinois de Zhejang News dénonçait un directeur d'école qui avait arbitrairement annoté le dossier personnel d'une institutrice de la mention *moralement décadente*. Offusquée mais dépourvue de tout moyen de rectification ou de contestation, l'institutrice a dû se résigner à quitter son emploi. Le titre de l'article *Protection des données : le droit chinois est encore aveugle* est révélateur d'un changement d'état d'esprit. Autre signal positif : le professeur Zhou Honhua de l'Institut de droit constitutionnel et administratif de l'Académie chinoise des sciences sociales vient d'élaborer un avant-projet de loi sur la protection des données, à l'objectif de parer aux nombreuses violations de la sphère privée sur Internet. Mieux, des travaux préparatoires officiels auraient débutés[1]. Il est vrai que des modèles « made in China » sont à portée de main : Taiwan et Hong-Kong[2] ont déjà légiféré sur la protection des données.

---

[1] *Falü Yu Shenghao 2005/288*
[2] *Personal Data (Privacy) Ordinance (Cap. 486).*

3. Ce bref examen de l'impact des différences de système juridique sur l'adoption d'un régime commun de la protection des données montre que ces obstacles sont soit loin d'être insurmontables : **si résistances, il y aura, c'est moins au niveau du contenu général des normes, mais plutôt au niveau de leur implémentation**. **Et là les différences politiques, économiques ou culturelles peuvent menacer, voire plomber une exécution uniformes des obligations internationales contractées.**

3.1. Je passerai rapidement sur **les différences d'ordre politique** pour simplement rappeler que le droit international peut être une opération de relations publiques. Nombres de régimes dictatoriaux ou de façade démocratique ratifient à tour de bras des textes flatteurs pour les droits de l'Homme dans le seul but de donner un signal fort de respectabilité. La Convention des Nations Unies de 1966 contre le racisme et la discrimination nous en donne un exemple : tous les États communistes d'alors se sont hâtés de la ratifier afin de faire bonne figure auprès des pays du tiers-monde.

Espérons donc que la mise en place d'un régime de haute protection des données en Tunisie ne soit pas purement opportuniste ; on peut toutefois en douter : on sait que le président Tunisien BEN ALI fait la vie dure à toute velléité d'opposition. Et la récente loi sur la protection des données a quelque relent d'autoritarisme : elle n'accorde aucune exception en faveur de la presse; quant à la Commission de la protection des données, elle jouit d'une indépendance relative : ses membres doivent leur nomination au seul président.

Différence politique encore, avec la fameuse juridiction constitutionnelle américaine. Risquant à tout moment les foudres du premier juge venu, les lois ont aux États-Unis un statut précaire. Une future loi sur la protection des données dans le secteur privé, de par les contraintes qu'elle imposera généralement dans la collecte et la diffusion d'informations, sera mesurée à l'aune de la toute puissante liberté d'expression. La décision FCC c/West,[1] prise en 1999 par une cour d'appel fédérale fait craindre des difficultés : l'espèce concernait une loi fédérale qui interdisait aux opérateurs de téléphonie d'utiliser les données personnelles de leur clients à des fins de marketing sans avoir obtenu leur accord préalable (système dit de l'opting-in). Après avoir relevé que « *Privacy is not an absolute good* » et après avoir souligné que les règles de protection des données contribuent à une baisse de productivité et à une augmentation des coûts, les juges fédéraux ont annulé l'obligation du consentement préalable.

3.2. Restons aux États-Unis, car ce pays illustre à merveille **l'impact des différences économiques** sur un éventuel régime commun de la protection des données, et le conflit qu'il peut engendrer avec la sacro-sainte liberté d'entreprendre.

L'*American way*, c'est la bride laissée libre aux forces du marché ; si régulation il doit y avoir, elle ne se conçoit que volontaire (c'est l'autorégulation) ou contractuelle (conventions entre les opérateurs économiques et les consommateurs p.ex.) ; l'État se tiendra sur la réserve et n'interviendra qu'en ultime ressort. Il y a plus : pour les

---

[1] *182 F.3d 1224. Pour plus de détails, voir R. Cain, Global Privacy Concerns and Regulation : is the United States a World apart?, International Review of Law, Computers and Technology 2002, 28ss.*

Américains, le corollaire nécessaire d'un marché libre, c'est la libre circulation de l'information ; autrement dit du *free flow of information* dépend le développement du commerce et partant le progrès. D'où une profonde réticence à protéger les données dans le secteur privé. Comme l'a dit en 1977 déjà le sénateur Mc GOVERN :

> « One way to « attack » a nation such as the United States which depends heavily on information and communications is to restrain the flow of information – cutting off contact between the headquarters and the overseas branches of a multinational firm; taxing telecommunications crossing borders, building information walls around a nation"[1].

Cela dit, réticence ne rime pas avec hostilité.

D'abord une certaine régulation du secteur privé existe, même si elle demeure à la fois rudimentaire et éclatée, affectant surtout les domaines de la santé, des télécommunications et des services financiers[2]: et encore, le peu qu'il y a souffre d'une absence de coordination, et surtout de l'absence de toute surveillance par une agence gouvernementale indépendante et dédiée[3]. C'est d'autant plus regrettable que les États-Unis ont été le berceau de l'administration polycentrique : les agences indépendantes y fleurissent comme nulle part ailleurs.

Mais le vent pourrait tourner soudainement. Depuis peu une réglementation du secteur privé n'est plus réclamée par les seules organisations de consommateurs, une entité administrative a pris le relais : la Federal Trade Commission, l'autorité indépendante chargée de réguler le commerce entre les États fédérés. La FTC a dressé, voici quatre ans, un bilan catastrophique de l'approche minimaliste américaine, relevant que l'autorégulation n'a pas donné satisfaction dans le monde volatil d'Internet. La FTC déplore aussi que les codes de conduite édictés par les entreprises commerciales sont touffus et rédigés dans un jargon juridique incompréhensible par Monsieur tout le monde[4]. Sera-ce assez pour inciter le Congrès à assujettir le secteur privé ? je le pense. Mais le lobby industriel demeure à l'affût ; il fera tout pour affaiblir le régime proposé, comme il l'a fait avec succès en matière de lutte contre le *spamming* : les États-Unis ont consacré le principe de *l'opting-out*[5] au contraire de l'Union européenne qui a choisi *l'opting in*[6], plus favorable aux consommateurs.

---

[1] *Cité par P. Regan, p. 260.*

[2] *Voir par exemple le Driver's Privacy Protection Act de 1994 ou le Financial Services Modernization Act of 1999. En outre aux États-Unis, la protection des données ne date pas d'hier : en 1973 déjà le Département du commerce avait développé des* fair information practices *destinés à réguler le traitement de données des consommateurs ; au début des années, il s'est engagé sans compter pour le respect par les plus grandes entreprises américaines des lignes directrices de l'OCDE (en vain sur 750 grandes entreprises contactées seules quelque 150 ont suivi les mot d'ordre)*

[3] *Le Privacy Act ne vise que les instances fédérales.*

[4] *J. Wakana, The future of Online Privacy : a proposal for international legislation, Loyola of Los Angeles International and Comparative Law Review 2003, p. 165 et 168..*

[5] *CAN-SPAM Act 2003, sec. 5.*

[6] *Directive CE 2002/58, art. 13*

3.3. J'en viens finalement aux **différences culturelles** ; une me paraît capitale : **la différence entre pays où l'on cultive le secret et ceux où l'on cultive la transparence**. Dans ce dernier groupe on retrouve les États-Unis (on songe au *Freedom of information Act* de 1966), mais aussi la Finlande et surtout la Suède qui depuis 1766 déjà permet à tout un chacun de consulter les documents détenus par les autorités. Entre droit d'accès aux documents administratifs et protection des données, le conflit était programmé. Et les pays qui cultivent l'ouverture ont tranché en donnant la priorité à la transparence, instrument central de contrôle et de participation à la vie publique.

Ainsi en Suède, l'article 8 de la loi sur la protection des données souligne que ce texte ne fait pas obstacle au droit d'obtenir des informations à caractère personnel garanti par la loi constitutionnelle sur la presse. La Finlande a fait de même mais avec un peu plus de nuance : tout en soumettant au régime de la transparence la communication d'informations personnelles contenues dans des fichiers (automatiques et manuels)[1], elle introduit quelques restrictions afin de prévenir un emploi abusif des données obtenues: ainsi, par exemple, l'autorité requérante peut refuser de procéder à des nomenclatures particulières ou à des consultations parallèles de fichiers qui porteraient atteinte à la vie privée des personnes concernées. Cette cautèle vise tout particulièrement la constitution de profils par de la personnalité par interconnexion[2].

3.4. Autre facteur de résistance d'ordre culturel : le chauvinisme, et **le chauvinisme juridique** plus particulièrement : l'ordre juridique se révèle en effet être un vecteur d'identité nationale[3]. Á tel point que certains États ont refusé de recevoir des règles juridiques, pourtant adéquates, au motif qu'elles proviennent de pays mal vus. Une attitude négative qui ne doit pas être sous-estimée lorsque l'on discute régime commun de la protection des données : l'institution est perçue comme occidentale, européenne par excellence. Des blocages peuvent donc survenir pour cette simple – mais pas bonne – raison.

4. Le temps pressant, je passerai rapidement en revue **les facteurs d'intégration susceptibles de contrecarrer les freins posés par les différences d'ordre culturel, politique, juridique ou économique**.

4.1. Premier facteur d'intégration : un besoin accru de protection internationale dû à la croissance fulgurante des réseaux de la communication en ligne. La protection des données est née dans les années soixante de l'essor des ordinateurs et des dangers qu'il faisait courir à la vie privée ; elle est en train de trouver une nouvelle justification avec le développement d'Internet ; on sait qu'Internet a considérablement amplifié les dangers d'atteinte à la vie privée ; le cyberespace se moquant des réglementations nationales, il est devenu impératif de définir des standards communs régissant tous les aspects de la communication à l'échelle planétaire. Ainsi, des règles uniformes ont déjà été édictées pour combattre le

---

[1] *Voir l'art. 8 in fine* Personuppgiftslag.
[2] *Art. 16 al. 3 et 18 al. 1* Lag om offentlighet i myndigheternas verksamhet.
[3] *Pour plus de détails, voir Impérialisme et chauvinisme juridiques, Publications de l'Institut suisse de droit comparé no 48, Zurich 2002.*

piratage des œuvres sur Internet ; il en va de même, avec la convention sur la cybercriminalité, en matière de lutte contre la pédopornographie et de sauvegarde de l'intégrité des systèmes informatiques (répression du hacking notamment). Le moment est donc propice pour lancer le débat autour d'un régime universel de la protection des données.

4.2. Deuxième facteur d'intégration : l'effet extraterritorial des principes de protection des données dus aux clauses interdisant l'exportation de données vers des États qui n'accorderaient pas une protection adéquate. Une implémentation plus conséquente et systématique de clauses, par la Commission européenne notamment, serait susceptible tirer le niveau de la protection des données vers le haut et de favoriser une vision commune. Les *safe harbor principles* négociés entre les États-Unis et l'Union européenne, peuvent certes prêter le flanc à la critique, ils ont eu au moins le mérite de sensibiliser comme jamais les milieux politiques et les entreprises américaines à la protection des données.

4.3. Troisième facteur d'intégration : l'existence d'un organisme mondial susceptible de fonctionner comme moteur d'intégration. Á ce jour pareil organisme moteur faite encore défaut, mais deux organisations internationales peuvent entrer en considération : l'Union internationale des télécommunications, qui patronne les « Sommets mondiaux de la société de l'information », et partant est soucieuse des enjeux des nouvelles technologies de l'Information et les Nations Unies. Cette dernière organisation, plus sensible à la dimension droit de l'Homme, serait idoine : la matière ne lui est pas inconnue, en 1990 déjà elle avait adopté des « lignes directrices pour la réglementation des fichiers de données personnelles automatisés ». Quelque soit l'organisation choisie, sa mission ne se bornera pas à élaborer des règles communes : elle devra aussi à assurer leur respect par le biais de mécanismes de surveillance (de monitoring) adéquats.

5. Au début de cet exposé, j'avais modifié mon titre pour souligner le fait que **la consécration d'un régime commun de la protection des données a son prix. Reste maintenant à le fixer.**

Un régime universel de la protection des données n'a d'avenir que si vous avez la sagesse de résister à la tentation de l'unification des règles, pour vous contenter d'un objectif moins ambitieux mais plus facile à atteindre : l'harmonisation.

Il s'agira de poser par le biais d'un instrument international contraignant – il va sans dire que le temps de la soft law est aujourd'hui révolu – quelques principes fondamentaux, principe de loyauté, de transparence, de proportionnalité, de finalité et de sécurité du traitement, droit d'accès, indépendance de l'autorité nationale de surveillance ; j'en passe et des meilleurs. Ces principes, il appartiendra aux États parties les mettre en œuvre tout en restant en phase avec leur tradition juridique, économique ou culturelle. C'est la clef du succès.

Le prix à payer n'est donc autre qu'un certain respect de la différence.

3. L'approche américaine : la régulation par le congrès, le marché et le juge

M. Robert GELLMAN
Avocat auprès de la cour suprême de Pennsylvanie
Expert-conseil en protection des données et vie privée

Mme. Suzanne INNES-STUBB
Avocate, White and Case LLP, Bruxelles

M. Robert GELLMAN
Avocat auprès de la cour suprême de Pennsylvanie
Expert-conseil en protection des données et vie privée

Intervention en anglais traduite en français.

Protection des données personnelles : la démarche américaine

Introduction

La méthode américaine de régulation de la protection des données personnelles est parfois qualifiée d'approche sectorielle. Elle s'oppose à l'approche systématique adoptée par la plupart des autres pays. Une approche systématique repose en général sur des normes complètes de protection inspirées des pratiques de l'information loyale (Fair Information Practice – FIP's) et traduites dans une législation applicable à presque tous les types de données personnelles et de détenteurs de fichiers. Un autre trait important d'une approche systématique est l'institution d'une autorité indépendante de protection des données.

Une appréciation positive de l'approche sectorielle des États-Unis met l'accent sur le choix réfléchi des sujets traités et de la méthode de la régulation. L'Amérique régule des activités et des informations pour protéger les données personnelles seulement quand un besoin clair et spécifique a été identifié. Normalement c'est au marché de résoudre les problèmes et la régulation n'intervient que lorsque tout le monde reconnaît que le marché a échoué, que les règles ont été élaborées de manière incohérente ou que la régulation serait plus efficace. Des règles de protection des données sont alors faites sur mesure en fonction du type de données personnelles et des catégories de responsables de fichiers qui gèrent et utilisent ces données. L'application de ces règles repose sur des institutions existantes ayant l'expérience de la régulation. Le souci de la protection constitutionnelle de la liberté d'expression est aussi une caractéristique récurrente des débats sur la protection des données auxÉtats-Unis.

Une vision négative de la régulation de la protection des données à l'américaine souligne que les lois et les politiques de protection des données naissent de crises, de scandales ou d'efforts non coordonnés de législateurs individuels. Une partie seulement des informations personnelles sont soumises à une quelconque régulation, sans aucune vision politique d'ensemble et avec beaucoup de lacunes dans la couverture, particulièrement pour les données du secteur privé. Les lois sont souvent basées sur un sous-ensemble des Pratiques de l'Information Loyale (Fair Information Practices) mais toutes les lois n'utilisent pas les mêmes éléments de ces pratiques ou ne le font pas de la même manière. Les mécanismes assurant le respect des lois varient de manière significative d'une législation à l'autre et les efforts pour appliquer ces lois sont souvent inexistants ou épisodiques. La mise en application (*enforcement*) à l'initiative des personnes concernées par les traitements de données est souvent impossible ou impraticable. Les nombreuses institutions qui ont en charge une forme de contrôle de la protection des données ou un rôle dans l'application des lois ont une autorité restreinte et assurer le respect de la protection des données est pour toutes les agences ayant la mission d'assurer le respect des législations, au mieux, une fonction secondaire. Aucune institution n'a une large responsabilité pour définir une politique de protection des données, la contrôler et la faire appliquer.

Le présent exposé décrit les principaux éléments de la régulation à l'américaine de la protection des données. Plutôt qu'un catalogue complet de la législation, de la jurisprudence et d'autres aspects, est proposé un choix d'exemples concernant les caractéristiques, les lois, les politiques et les institutions.

I. La portée des lois américaines de protection des données

Au niveau fédéral

1. La Constitution

Les protections données par la Constitution en matière de protection des données sont d'une portée limitée et incertaine.
Dans sa décision Whalen v. Roe, la Cour suprême a décrit ses propres décisions en la matière comme assurant la protection de deux sortes d'intérêts[1]. L'un est l'intérêt individuel d'éviter la révélation d'éléments de la vie personnelle et l'autre est l'intérêt de pouvoir prendre certaines décisions en toute indépendance (par exemple dans les domaines touchant au mariage, à la procréation, à la contraception, aux relations familiales, à l'éducation) et les cours inférieures ont tiré des conclusions différentes des décisions de la Cour suprême.
Les normes constitutionnelles donnent des droits individuels à l'égard de l'État mais non à l'égard d'autres individus ou personnes morales. Ainsi la protection du 4ème amendement contre des perquisitions et des saisies excessives limite seulement le pouvoir de l'État de perquisitionner le domicile et de saisir des documents privés. Elle ne s'applique pas quand l'État obtient des informations personnelles auprès des

[1] *429 U.S. 589 (1976).*

tiers détenteurs de fichiers[1]. Dans le monde d'aujourd'hui où banques, opérateurs de télécommunications et fournisseurs d'Internet sont parmi les nombreux organismes qui ont des fichiers sur les individus, les protections constitutionnelles ont perdu de leur force.
D'autres dispositions de la Constitution traitent d'autres aspects de la protection de la vie privée mais pas de manière directe et complète. Si la protection des données n'est pas étrangère à la Constitution, on trouvera presque toutes les garanties soit dans la loi soit dans le droit coutumier. L'interdiction posée par la Constitution de limiter la liberté d'expression crée quelques tensions avec la protection des données mais les tribunaux n'ont pas exploré de manière approfondie ce conflit.

2. La régulation des activités de l'État fédéral

La principale loi de protection des données pour le gouvernement fédéral est **le Privacy Act de 1974**[2]. Cette loi s'applique à toutes les agences fédérales ainsi qu'à une catégorie limitée de contractants privés.

La loi d'origine contraste avec la plupart des autres lois américaines de protection des données car elle est le produit d'un processus politique détaillé. Un comité consultatif créé en 1973 a étudié les effets de l'usage public et privé croissant des traitements automatiques de données contenant des informations sur les individus[3]. L'une des productions de ce comité fut la publication du premier code des pratiques de l'information loyale (Code of Fair Information Practices), un code dont les Européens se sont plus tard inspirés comme base de leurs lois générales de protection des données.

Un second ensemble de recommandations ont directement conduit à la promulgation du Privacy Act de 1974. La loi comprend l' ensemble complet de Pratiques de l'Information Loyale, y compris les obligations relatives à la transparence, aux droits d'accès et de rectification, à la limitation de collecte des données, de leur usage et de leur divulgation, à la sécurité et à la qualité des données, à la responsabilité.
Les agences fédérales ont opéré sous cette loi pendant plus de trente ans avec peu de problèmes significatifs, même s'il apparaît que le respect du Privacy Act est souvent indifférent.

Le Privacy Act pose quatre problèmes principaux. Le premier est que le modèle technologique de la loi est l'ordinateur central. La loi n'est pas bien adaptée aux ordinateurs personnels, aux bases de données ou à Internet. Le second est que la loi s'applique à la plupart mais pas à toutes les informations personnelles que l'administration détient. La distinction entre les informations soumises à la loi et celles non soumises dépend de la manière dont ces informations sont extraites, une

---

[1] *…United States v Milla 435 (1976) (un individu ne bénéficie d'aucune protection de ses données contenues dans les fichiers d'une banque). Le Congrès a partiellement contredit cette décision dans le Financial Privacy Act of 1978… Toutefois cette loi comporte de nombreuses exceptions et limitations et le niveau réel de protection est discutable.*
[2] *5 U.S.C. § 552a.*
[3] *Secrétaire du comité de conseil sur les systèmes automatisés de données personnelles, archives, ordinateurs, et les droits des citoyens, (1973) (Ministère de la santé, de l'éducation et de l'aide sociale des États-Unis), au http://aspe.os.dhhs.gov/datacncl/1973privacy/tocprefacemembers.htm.*

distinction qui n'a plus beaucoup de sens aujourd'hui. Le troisième est que les contrôles prévus par la loi sur la divulgation des informations ne sont efficaces que de manière marginale. Les agences peuvent facilement contourner les règles relatives au principe de finalité. Le quatrième est que la loi est difficile à mettre en application à l'initiative d'individus, bien que ce ne soit pas impossible.
Malgré les lacunes de cette loi, elle pourrait probablement être considérée comme apportant un niveau adéquat de protection au regard des normes européennes si elle ne comportait pas deux restrictions majeures. En premier lieu, la loi ne donne pas de droits aux personnes de nationalité étrangère. Seuls les citoyens américains et les résidents étrangers ont des droits.
En second lieu, la loi ne restreint pas les transferts de données. Si l'administration divulgue des informations personnelles à quelqu'un d'autre qu'une agence fédérale, ces informations tombent en dehors de la protection du Privacy Act.

3. La régulation du secteur privé dans le domaine de la protection des données

La régulation au niveau fédéral du secteur privé est limitée aux responsables de fichiers expressément couverts par la loi[5]. En l'absence d'une loi spécifique, il est probable qu'aucune régulation formelle de la protection des données n'existe. Beaucoup de fichiers utilisés dans les transactions commerciales courantes restent sans protection de données personnelles. Des commerçants de tous types, des éditeurs de magazines, des restaurants, des agences de voyage, des organismes caritatifs, des organisations sans but lucratif et bien d'autres sont souvent libres de collecter, d'utiliser ou de diffuser des informations personnelles qu'ils obtiennent des individus sans aucune règle fixée par la loi. Beaucoup font seulement cela. Des lois générales de régulation – comme dans les domaines de la banque et des télécommunications – fournissent parfois au consommateur une protection limitée de leurs données personnelles à travers des obligations d'information ou des droits d'accès. Le nombre de ces législations n'est pas négligeable, cependant on mettra ici l'accent sur celles dont l'objectif principal est d'assurer la protection des données personnelles et sur leurs lacunes.

- **Fair Credit Reporting Act « FCRA » (1970)**. La première loi fédérale moderne de protection des données personnelles a été la loi sur les rapports relatifs à la situation financière des individus [6](NDT ces rapports portent notamment sur l'endettement des personnes et sont constitués par des aentreprises privées). Bien que cette loi ait devancé la formulation du code des pratiques de l'information loyale (Code of Fair Information Practices), elle en contient tous les éléments. L'origine du vote de la loi se trouve en grande partie dans les efforts d'un sénateur qui a organisé des auditions au Congrès qui ont montré l'importance des rapports sur la situation financière des individus (« Credit report ») dans leur capacité à obtenir un crédit, un emploi ou une assurance et l'absence de droits des individus à l'égard de ces rapports.
En vertu du FCRA, les consommateurs ont des droits relatifs aux fichiers tenus par les agences de notation financière et utilisés par leurs clients.

---

[5] *Les professeurs Schwartz et Reidenberg décrivent les lois concernant le secteur privé comme tournant autour de « droits étroits comme réponse à des thématiques discrètes », Paul M. Schwartz…*
[6] *15 U.S.C. § 1681 et seq.*

Le droit d'accès a été récemment renforcé et les consommateurs ont maintenant le droit d'avoir une fois par an gratuitement une copie de leur rapport. La loi inclut aussi de meilleures protections pour les victimes de vols d'identité. Cependant quand les professionnels utilisent des informations similaires mais en provencance d'autres sources d'information (par exemple leurs propres fichiers ou en provenance d'Internet), il y a peu de chances que la loi FCRA s'applique. Sur la base du FCRA ou d'autres lois, le partage d'informations entre filiales d'un groupe est soumis à une réglementation faible ou inexistante. Comme de plus en plus d'informations sur les consommateurs sont accessibles en ligne à travers des moteurs de recherche ou disponibles au sein même d'une entreprise (particulièrement du fait des fusions au sein des sociétés financières), l'importance du FCRA pourrait bien décliner en proportion du développement de sources de données échappant à toute règle.
Une seconde limite est qu'une partie de la fiche individuelle de situation financière (« credit file »), connue comme les informations de l'en-tête de la fiche (« credit trader information ») n'est pas soumise à la réglementation à cause d'une décision prise il y a plusieurs années par la Federal Trade Commission qui est l'agence responsable du suivi du FCRA. Cet en-tête comprend le nom, l'adresse, les adresses précédentes, le numéro de téléphone, la date de naissance et le numéro de sécurité sociale. Des listes de la plupart des Américains et de la plupart des ménages peuvent être élaborées uniquement à partir de ces données et la plupart de ceux qui vendent de telles listes ne sont pas soumis à une réglementation de protection des données. Des sphères entières du commerce des données existent seulement à cause de cette faille de l'en-tête de la fiche de crédit.

- **Family Educational Rights and Privacy Act[7] (1974)**

Cette loi donne des droits d'accès et limite la diffusion des données des fichiers des étudiants tenues par les écoles et universités bénéficiant de fonds de l'État fédéral. La loi n'offre aucune protection pour les fichiers concernant le corps enseignant, le personnel administratif, les diplômés ou les donateurs de n'importe quelle institution éducative. Cette loi trouve son origine dans un amendement de séance d'un sénateur, voté sans auditions préalables et sans débat substantiel.

- **Cable Communications Policy Act[8] (1984)**

Cette réglementation d'ensemble de l'industrie de la télévision par câble offre des protections pour les données personnelles dont des restrictions à la diffusion des données des fichiers concernant les programmes télévisés regardés par les abonnés. Cependant les consommateurs qui ont accès aux programmes de télévision par satellite n'ont pas eu de protection légale similaire jusqu'au vote d'une loi nouvelle, plus de vingt ans après[9]. Si un nouveau mode de diffusion de la télévision apparaissait, il faudrait une autre décision du Congrès pour étendre la protection des données personnelles aux téléspectateurs concernés.

- **Video Privacy Protection Act[10] (1988)**

---

[7] *20 U.S.C. § 1232g.*
[8] *47 U.S.C. § 551.*
[9] *47 U.S.C. 338.*
[10] *18 U.S.C. §2710.*

Pendant une audition agitée au Sénat pour la confirmation d'un candidat au poste de juge à la Cour suprême, un journaliste dévoila le titre des films que le candidat avait loué dans un vidéoclub. Bien que cette révélation ne fut pas la cause du rejet de la candidature, certains membres du Congrès déplorèrent que ces fichiers ne soient pas protégés, peut-être par crainte de voir leurs propres locations rendues publiques. En résulta la loi sur la protection des données relatives à la vidéo qui apporte une protection réduite pour les fichiers d'achats et de location de vidéos. Il n'y a cependant aucune législation équivalente pour les informations relatives aux achats de livres, de magazines ou d'autres produits similaires.

- **Driver's Privacy Protection Act[11] (1994)**

Cette loi limite la diffusion et l'utilisation des données des fichiers de permis de conduire et d'immatriculation des véhicules à moteur tenus par l'administration. Elle trouve son origine, entre autres, dans le meurtre d'une actrice de télévision par un admirateur mentalement déséquilibré qui avait obtenu son adresse privée grâce aux registres publics d'immatriculation. Les États fédérés ont leurs propres lois pour ces fichiers mais ils doivent aussi se plier aux restrictions établies par la loi fédérale. Cette loi autorisait initialement une cession des données à des fins commerciales en l'absence d'opposition des conducteurs mais en 1999 un amendement voté sur l'insistance d'un sénateur a renversé le principe de sorte que la cession à des fins commerciales requiert maintenant le consentement exprès des intéressés. Alors que cette loi encadre les registres d'immatriculation des véhicules des états fédérés, aucun des nombreux autres registres publics n'est soumis, en ce qui concerne la protection des données, à une réglementation fédérale.

- **Children's Online Privacy Protection Act[12] "COPA"(1988)**

Cette loi fixe des règles régissant la collecte, l'enregistrement, l'usage et la diffusion des données personnelles obtenues en ligne d'enfants de moins de 13 ans. Cependant il n'y a pas de réglementation comparable au sujet des informations personnelles collectées auprès d'autres enfants de tous âges par téléphone, fax ou tout autre moyen.

- **Health Insurance Portability and Accountability Act[13] "HIPA" (1996)**

Cette loi fédérale a autorisé le ministère de la santé à émettre des règles de protection des données en matière de santé. Ces règles sont entrées en vigueur en 2003[14]. La réglementation s'applique aux fournisseurs de soins et aux organismes de prévoyance et de compensation. Elle prévoit la transparence, les droits d'accès et de rectification, des limites à l'usage et à la diffusion des données et des règles de responsabilité mais beaucoup de protections sont assorties d'exceptions ou de limites procédurales. De plus beaucoup d'organismes (organismes de contrôle de la loi, organismes de santé publique, organismes de surveillance de la santé, tribunaux, chercheurs), sont autorisés à obtenir des informations sans le consentement des patients concernés et ne tombent pas sous le coup de la réglementation. La loi ne restreint pas les traitements de données qu'ils font. D'autres grands organismes qui

---

[11] *18 U.S.C. § 2721 et seq.*
[12] *15 U.S.C. § 6501 et seq.*
[13] *42 U.S.C. §1320d-2 note.*
[14] *45 C.F.R. Parts 160 & 164.*

utilisent couramment des données de santé, parmi lesquelles les compagnies d'assurance vie, les fonds d'indemnisation d'arrêts de travail et des commerçants ne sont pas soumis à la réglementation fédérale de la protection des données de santé.

Lois des états fédérés et préemption fédérale

4. Protections constitutionnelles

Certaines constitutions d'États reconnaissent expressément la protection des données personnelles comme un droit fondamental. La plus forte protection par une constitution est assurée en Californie où en 1974, un référendum a fait de la protection des données l'un des quelques droits inaliénables[15]. La Cour suprême de Californie a décidé en 1994 que la protection constitutionnelle s'appliquait aussi bien au secteur public qu'au secteur privé[16].
Le véritable effet de la règle constitutionnelle reste encore obscur. Les protections constitutionnelles prévues dans d'autres états n'apparaissent en tout cas pas aussi solides qu'en Californie.

5. Les lois des États

Les lois des États varient énormément d'un État à l'autre. Environ un quart des États ont des législations générales de protection des données applicables aux fichiers de l'État. Les lois sur la protection des données de santé sont nombreuses mais leur portée, leur qualité et leur valeur ne peuvent en être facilement mesurées. Certains États ont des lois plus modernes de protection globale des données de santé, certains n'en ont pas et d'autres ont des lois à l'ancienne qui ne correspondent pas à la complexité des traitements des données de santé. Tous les États ont des dizaines de lois qui ont un impact sur ces traitements mais les lois diffèrent selon les professions concernées (médecins, pharmaciens, psychiatres) selon les organismes (assureurs, hôpitaux, cliniques) et le type de fichier (données génétiques, abus de substances toxiques, santé mentale). Aucun État n'a le même modèle de régulation pour les traitements de données de santé. Les textes réglementant les fichiers à usage commercial sont épars et la plupart de ces traitements ne sont pas soumis à une quelconque réglementation par les états.

6. Les registres publics

Les États et collectivités locales ont de nombreux fichiers sur les individus. Parmi lesquels les fichiers d'immatriculation des véhicules à moteurs, les cadastres, les fichiers de taxes foncières, les listes électorales, les registres d'autorisation d'exercer un métier, les fichiers de permis de détention d'armes et de contraventions, ceux concernant les déclarations de détention d'intérêts financiers (dans un but éthique), les permis de chasser ou de pêcher et bien d'autres[17]. Bien que les politiques varient d'un État à l'autre et d'un traitement à l'autre, beaucoup de ces fichiers sont des

---

[15] *Cal. Const. at I, § 1.*
[16] Hill v. NCAA*, 865 P.2d 633 (Cal. 1994).*
[17] *Cf Robert Gellman,* Public Records: Access, Privacy, and Public Policy*, 12 Government Information Quarterly 391-426 (1995).*

registres publics qui sont disponibles en tout ou partie pour des usages répondant à l'intérêt public. Les sociétés privées qui font commerce des données personnelles font usage à grande échelle de ces fichiers pour développer des profils d'individus et de foyers. La disponibilité permanente de ces fichiers rend possible un traçage, tout au long de la vie, des gens, de leurs adresses, de leurs activités financières et autres de leurs habitudes de vie. Les lois fédérales restreignent seulement la diffusion de l'information sur les véhicules à moteur. Mais, à cause des problèmes de vol d'identité, des États se sont mis à revoir leurs politiques de mise à disposition de certains de ces fichiers.

7. Préemption fédérale

Le gouvernement fédéral et les États partagent souvent la compétence législative sur beaucoup d'aspects du commerce. La réglementation de la protection des données est parfois assurée par les États, parfois au niveau fédéral, parfois par les deux, parfois par aucun des deux. Le niveau fédéral a souvent autorité pour préempter les initiatives législatives d'un État fédéré et cette préemption fédérale de la protection des données personnelles est une tendance croissante[18]. Les entreprises sont souvent opposées à une législation de protection des données au niveau des États comme au niveau fédéral. Mais après que les États ont commencé à adopter des lois, le monde des affaires quelquefois est en faveur d'une loi fédérale assurant un niveau de protection plus faible qui prenne le pas sur toutes les lois d'États. L'argument en faveur d'une loi fédérale est qu'il serait plus facile de se mettre en conformité avec une loi uniforme. Les États et les défenseurs de la protection des données personnelles s'opposent en général à la préemption fédérale au nom du respect du fédéralisme et parce que les lois fédérales offrent souvent moins de protection des données personnelles que les lois des États qu'elles préemptent. La tendance actuelle en matière de protection des données est la préemption totale ou partielle des lois des États par la loi fédérale.

Conclusion : l'approche sectorielle américaine produit des lois de protection des données qui offrent des protections limitées à des catégories étroites d'informations personnelles avec des différences dans la nature de la protection d'une loi à l'autre. Des catégories semblables d'informations peuvent être soumises à des règles largement disparates allant d'une protection forte à une absence de protection. Beaucoup de traitements de données personnelles mis en œuvre par des organismes du secteur privé ne sont pas accessibles au public et ne sont soumis à aucune règle de protection. Certaines informations personnelles détenues par certains responsables de traitements font l'objet d'une réglementation tandis que des informations comparables lorsqu'elles sont dans d'autres mains y échappent. Il peut être difficile même pour des avocats de savoir quelle loi de protection des données, s'il y en a une, s'applique à des informations personnelles. Il est rare qu'une règle de protection

---

[18] *Une loi californienne qui donnait de meilleures protections des fichiers financiers a été récemment tenu pour être préemptée par la loi fédérale Fair and Accurate Credit Transactions Act of 2003, Pub. L. 108-159, 117 Stat. 1952.* American Bankers Association v. Gould, *412 F.3d 1081 (9th Cir. 2005); en detention provisoire* American Bankers Association v. Lockyer *2005 U.S. Dist. LEXIS 22437 (E.D. Cal., Oct. 4, 2005).*

suive des fichiers lorsqu'ils sont transférés du détenteur initial à un autre usager. Des protections constitutionnelles à l'égard des autorités publiques existent mais ces protections sont souvent étroites et leur champ incertain.

II. Les mécanismes assurant le respect de la vie privée et des données personnelles

1. L'action en responsabilité délictuelle pour atteinte à la vie privée (droit coutumier)

Lorsqu'il n'existe pas de texte législatif, les personnes peuvent cependant trouver une protection dans l'action en responsabilité délictuelle (tort). La jurisprudence américaine sur la vie privée s'est ainsi développée depuis le célèbre article de la Harvard Law Review en 1890 qui proposait le développement d'une doctrine judiciaire dans ce domaine[19]. Les quatre atteintes à la vie privée les plus souvent ainsi reconnues sont: 1) l'intrusion dans la solitude d'un individu 2) le fait de rendre public des faits privés 3) le fait de diffamer un individu de manière très choquante pour une personne raisonnable 4) un usage non autorisé à des fins commerciales de l'identité d'un individu[20].

La valeur de ces jurisprudences sur l'atteinte à la vie privée pour la protection des données personnelles est loin d'être claire[21]. En raison du caractère souvent non apparent de l'échange commercial, de la conservation et de l'usage des informations personnelles, les personnes concernées savent rarement à quelle fréquence les commerçants et ceux qui vendent des données les recueillent, utilisent et partagent les informations personnelles. Le manque de transparence fait que les consommateurs ont du mal à envisager d'utiliser les recours judiciaires. Les recours ont d'ailleurs d'autres limites qui leur sont inhérentes. La réparation qui pourra être obtenue sera souvent limitée à celle des seuls préjudices financiers. La plupart des principes d'une information loyale ne peuvent être directement invoqués à travers ce type d'action judiciaire. Il y a peu de chance que la définition classique des atteintes à la vie privée conduise un responsable de fichiers à publier la description du traitement de données, à respecter les règles de qualité des données, à permettre aux individus l'accès et la rectification ou à restreindre les usages internes des données.

2. Les mécanismes prévus dans les textes législatifs pour en assurer le respect

Il y a différentes manières d'assurer le respect d'un texte de protection des données. Une grande partie, mais pas la totalité des lois spécifiques précitées, donne aux

---

[19] *Louis D. Brandeis & Samuel D. Warren,* The Right to Privacy*, 4 Harvard Law Review 193 (1890).*

[20] *3 Restatement (Second) of Torts §652A et seq. (1977).*

[21] *Diane L. Zimmerman,* Requiem for a Heavyweight: A Farewell to Warren and Brandeis's Privacy Tort*, 68 Cornell Law Review 291, 334 (1983) ("Après quatre vingt dix ans d'évolution, les faits de protection de la vie privée du droit coutumier n'a pas réussi à devenir un moyen exploitable et efficace de recours pour les plaignants"); Fred H. Cate, Privacy in the Information Age, 90 (atteintes à la vie privée "offrent peu de protection pour les données personnelles.").*

individus un droit d'agir qui leur permet d'engager des poursuites en cas de violation. Cependant, même quand ces poursuites sont possibles, elles peuvent être difficiles à mener. Il est souvent difficile de prouver que l'on a subi des dommages dans ce type d'affaire et le faible montant des réparations qui peuvent être obtenues fait qu'il n'est pas aisé de trouver des avocats qui acceptent de soutenir l'action. Les lois fédérales récentes en matière de protection des données ont tendance à ne pas donner aux individus un droit d'agir.

Le Privacy Act de 1974 donne un droit à agir à condition que les dommages soient au minimum de 1 000$. Les règles de preuve des dommages sont très exigeantes et une récente décision de la Cour suprême a rendu encore plus improbable le succès de cette procédure[22]. Cela fait longtemps que cette voie a été reconnue comme inefficace. Le Privacy Act assure aussi son application à travers une sanction pénale punie d'une légère amende. En trente ans, ces sanctions pénales n'ont été que rarement utilisées.

Le Cable Communication Policy Act comprend un droit à agir des abonnés à la télévision par câble contre les câble-opérateurs. C'est le seul mécanisme pour assurer le respect de la loi. Dans la mesure où cette loi fixe des normes pour la transparence, la qualité des données, la définition d'une finalité, la limitation des usages et la participation des individus, le non-respect par un câble-opérateur de ces bonnes pratiques pouvant servir de base à des poursuites. Pourtant il est rare que de telles actions individuelles aient été couronnées de succès.

Le Driver's Privacy Protection Act comprend deux voies d'action civile en plus de la possibilité d'une action pénale. L'Attorney général des États-Unis peut chercher à infliger une amende civile à un État qui ne se conforme pas à la loi de manière substantielle. Un individu peut poursuivre une personne qui obtient, révèle ou utilise des informations personnelles tirées d'un fichier de véhicules à moteur dans un but inapproprié. L'État de Floride ne se conformait pas à la loi et des poursuites à titre privé furent engagés contre les sociétés qui continuaient à acheter des fichiers de conducteurs en violation de la loi fédérale[23]. La procédure n'est pas achevée mais les plaignants ont obtenu récemment une importante décision qui peut leur permettre d'obtenir des dommages et intérêts significatifs.

Souvent la seule option est de faire assurer le respect de la loi par l'administration. Le respect du Family Educational Rights and Privacy Act peut être assuré par le ministère de l'éducation en : 1) retirant les crédits à une école dépendant d'un programme fédéral 2) formulant une requête pour obtenir une injonction de se conformer à la loi 3) supprimant de l'éligibilité à recevoir à l'avenir des subventions. La loi dispose clairement que la suppression des subventions n'intervient qu'en dernier ressort. Les tentatives pour faire respecter la loi à travers un droit d'agir individuellement ont échoué[24].

---

[22] Doe v. Chao, *540 U.S. 614 (2004).*
[23] Kehoe v. Fidelity Federal Bank & Trust, *2005 U.S. App. LEXIS 18406 (11th Cir.).*
[24] Gonzaga University v. Doe, *536 U.S. 273 (2002).*

Les lois récentes de protection des données ont tendance à faire assurer le respect de la loi uniquement par l'administration plutôt que de donner aux individus un droit d'agir. Les avocats spécialisés dans le contentieux ne sont pas en odeur de sainteté chez le parti politique qui contrôle la Maison blanche et le Congrès et la création de nouvelles opportunités de faire des procès attire peu de soutien. Les entreprises qui sont soumises à des règles de protection de données s'opposent aussi en général au droit d'agir. Voici quelques-unes des lois récentes dont les individus ne peuvent obtenir le respect à travers une action judiciaire :

- Le Children's Online Privacy Protection Act prévoit que le respect de ses dispositions est assuré par la Federal Trade Commission et les Attorneys généraux des états. Les individus n'ont pas de moyen d'action individuelle.
- Le respect de la **loi Gramm-Leach-Bliley** qui réglemente les entreprises de services financiers est assuré par les régulateurs bancaires fédéraux, les autorités de contrôle des assurances des États et la Federal Trade Commission[25]. Au moins sept agences fédérales différentes ont le pouvoir pour veiller à l'application de la loi, ce qui reflète la diversité générale de la régulation du secteur bancaire. La loi ne prévoit pas de droit à l'action individuelle.
- **La loi CAN-SPAM de 2003** (The Controlling the Assault of Non-Solicited Pornography and Marketing Act) est considérée par certains comme une loi de protection des données. Elle prévoit que sont chargés d'assurer son respect plusieurs agences fédérales, les États et les fournisseurs d'accès Internet mais pas les individus. La loi fédérale a formellement éliminé les recours individuels prévus par quelques États.

- La législation sur la protection des données de santé résultant du Health Insurance Portability and Accountability Act prévoit des actions administratives et des sanctions pénales mais aucun droit à agir individuellement. Dans ses deux premières années d'application, aucune action administrative n'a été engagée. La sanction pénale a été employée uniquement pour poursuivre un voleur d'identité mais une nouvelle interprétation de loi par le ministère de la justice restreint de manière significative l'applicabilité de la sanction de sorte que beaucoup de détenteurs de données de santé ne pourront être poursuivis même s'ils font un mauvais usage de ces données[26].

De manière générale, l'action administrative a été, au mieux, occasionnelle. Le Wall Street Journal relatait récemment que la Federal Trade Commission reçoit chaque jour entre 1 000 et 2 000 plaintes au sujet de violation de la loi Do Not Call law[27]. Pourtant la Federal Trade Commission n'a engagé que quatorze poursuites et n'a infligé que quatre amendes. La Federal Trade Commission qui est aussi chargée de l'application de cette loi, a infligé une amende à deux entreprises seulement[28]. Dans

---

[25] *15 U.S.C. § 6805.*

[26] *Department of Justice, Office of Legal Counsel, Scope of Criminal Enforcement Under 42 U.S.C. § 1320d-6 (June 1, 2005) at http://www.usdoj.gov/olc/hipaa_final.htm.*

[27] *15 U.S.C. § 6101 note.*

[28] *Christopher Conkey,* Do-Not-Call Lists Under Fire: After Two Years and One Million Complaints, Only Six Federal Fines Have Been Issued, *Wall Street Journal, Sept. 28, 2005, D1.*

une autre affaire, la F.T.C. a engagé une action contre une entreprise qui a vendu sa liste de clients en violation de sa propre politique de protection des données. L'amende a été précisément le montant du profit qu'a tiré l'entreprise de la vente de la liste[29].

3. Autorégulation et normes professionnelles

Il est difficile d'évaluer l'autorégulation pratiquée par des groupes de professionnels. Certains groupes institués pour promouvoir le respect de normes de protection des données par les entreprises n'existent plus. Le Individual Reference Services Group ne fonctionne plus. Le Online Privacy Alliance maintient encore un site web mais rien n'y a été mis en ligne[30]. L'organisation ne semble pas être active. Le Privacy Leadership Initiative s'est dissout après quelques années. On peut penser que le principal objectif de certaines de ces organisations était de faire du lobbying contre le vote de lois de protection des données. Le Individual Reference Services Group par exemple s'est dissout après le vote de la loi Gramm-Leach-Bliley réglementant les institutions financières. Ce groupe a dit qu'il n'était plus nécessaire parce qu'il existait une législation de protection des données. Pourtant cette législation en général ne s'appliquait pas aux membres du groupe. Il semble que si le groupe s'est dissout, c'est en raison du manque de motivation de ses membres.
TRUSTe est une organisation indépendante, à but non lucratif qui gère des programmes d'auto-régulation, y compris un programme de label protection des données pour les acteurs de l'internet. Cette organisation est active et son label peut être trouvé sur beaucoup de sites web. Elle rend compte des plaintes qu'elle reçoit mais il est difficile de mesurer les résultats de cette procédure de plainte et son efficacité. Le site web indique pour l'année complète la plus récente (2004) qu'il n'y a eu ni investigations sur des membres de l'organisation ni exclusions de certains de ceux-ci[31].

Le Better Business Bureau propose aussi un programme de résolution des conflits portant sur la protection des données à trouver BBBOnLine Privacy Program. Quelques statistiques sont disponibles sur son site web[32] mais il y a peu de décisions publiées. Il n'y a pas assez d'informations disponibles pour évaluer le programme. Les autres programmes de labels ne fonctionnent plus.

Conclusion : De manière générale, l'efficacité des moyens d'assurer le respect des lois de protection des données aux États-Unis est sujette à caution. Alors qu'en théorie beaucoup de méthodes sont disponibles, les lois de protection des données font quelques fois autant pour limiter les actions que pour les encourager. Les moyens individuels d'action, qu'ils trouvent leur source dans le droit général ou dans les textes spécifiques, sont bien vus par la communauté des défenseurs de la protection des données mais les poursuites sont difficiles à mener, sont chères et l'obtention de réparations est rare. Faire la preuve du préjudice peut être difficile. Les

---

[29] http://www.ftc.gov/opa/2004/07/gateway.htm.
[30] http://www.privacyalliance.org.
[31] http://www.truste.org/consumers/watchdog_advisories/2004.php.
[32] http://www.bbbonline.org/privacy/dr.asp.

poursuites ont le plus de chance de réussite quand les faits sont suffisamment monumentaux pour ébranler un jury. La menace d'une poursuite peut être un outil modérément efficace pour assurer le respect de la loi mais les risques d'une publicité négative suscitée par une histoire d'honneur peut être plus efficace. D'un autre côté le lobbying agressif des milieux d'affaires contre le droit d'agir individuellement suggère que les poursuites sont redoutées par ces milieux. Le point de savoir si ces poursuites sont efficaces et coûteuses par les entreprises ou simplement embêtantes peut être discuté.

Les effets de l'intervention de l'administration pour assurer le respect de la protection des données ne sont pas clairs. L'agence qui a le plus de pouvoir est la Federal Trade Commission mais son champ d'intervention est restreint de manière significative. La FTC fait valoir qu'elle a des ressources limitées mais que ses actions occasionnelles donnent une véritable incitation aux entreprises à se conformer aux règles de la protection des données. Elle se saisit de peu d'affaires et inflige rarement des sanctions significatives aux contrevenants ou fournit aux consommateurs des solutions.

La preuve de l'efficacité des mécanismes mis en œuvre par le secteur privé, y compris les labels et les audits, est limitée. L'arrêt fréquent des activités des organisations instituées par les professionnels pour assurer le respect de la protection des données semble donner une indication très parlante du monde des affaires. Les programmes de labellisation et les activités des associations de commerçants sont financées par les entreprises qui les utilisent et il arrive que leurs programmes de résolution des conflits portant sur la protection des données ne fassent appel à aucune participation de personnes indépendantes et ne donnent lieu ni à un rapport ni à un audit.

D'une certaine manière, le mécanisme le plus efficace pour assurer le respect de la protection des données est peut-être le risque de publicité négative. Un incident relatif à des données personnelles qui est largement répercuté par les media sous forme de scandale peut produire les plus grands changements dans la loi et les pratiques. Par exemple, les récentes révélations de la presse sur les manquements à la sécurité et autres insuffisances dans le domaine de la protection des données commis par ChoicePoint et d'autres sociétés ont fortement retenu l'attention du public et du législateur. Ces révélations ont non seulement sensibilisé les entreprises à leur sécurité et aux risques juridiques qui sont liés mais elles ont aussi poussé beaucoup d'états à adopter de nouvelles lois obligeant la révélation des atteintes à la sécurité des données personnelles. Une législation fédérale est en préparation. Au final, cependant, les résultats de ces incidents sont plus d'activité et de législation pour traiter quelques éléments de la protection des données à la manière typiquement américaine : sans coordination et morceau par morceau.

Les organismes américains chargés de la protection des données

Les institutions qui contrôlent ou veillent à l'application de la protection des données aux États-Unis montrent la même diversité que celle-ci qui caractérise en général l'approche américaine de la protection des données. Des organismes sont créés ou se

voient assigner de nouveaux rôles sans beaucoup de réflexion préalable ou de coordination. Aucune autorité publique ne joue un rôle primordial ou ne dispose d'une compétence générale.

Administrations fédérales

1. L'Office Management and Budget

En raison de son rôle dans l'élaboration du budget du Président, l'Office of Management and Budget (OMB) est une agence puissante. Le Congrès a donné à l'OMB un rôle de contrôle du Privacy Act de 1974. Cependant les activités de gestion de l'OMB ont toujours été secondaires par rapport à ses fonctions budgétaires et la protection des données l'a peu mobilisé. Á une exception significative près, l'OMB affecte traditionnellement un seul de ses agents au moins aux dossiers de protection des données. OMB n'est pas une agence chargée d'assurer l'application des lois, on peut donc s'attendre à ce qu'elle joue un rôle opérationnel dans l'application des lois sur la protection des données ou qu'elle apporte de l'aide sur ces questions. L'OMB n'a qu'un rôle, rarement exercé, de contrôle des agences fédérales.
La seule période d'une attention plus développée du gouvernement aux questions de protection des données s'est produite durant l'administration CLINTON. CLINTON a nommé un conseiller pour la protection des données à l'OMB en mars 1999. Ce conseiller a joué un rôle dans le contrôle de l'application du Privacy Act de 1974 et a participé activement à d'autres dossiers et textes législatifs relatifs à ces questions. Toutefois l'administration Bush a supprimé ce poste quand elle arrive au pouvoir en janvier 2001 et toute cette politique de protection qu'avait entreprise le conseiller a disparu des préoccupations de l'exécutif. D'autres agences fédérales – principalement le Département d'État et le ministère du commerce – ont occasionnellement été impliqués dans des dossiers internationaux ou internes, mais ces activités se font par à-coup. Le ministère de la sécurité intérieure a désormais un rôle dans certains aspects internationaux de la protection des données liés à la lutte contre le terrorisme.

2. Les chargés de protection des données (Privacy Officers)

Certaines agences fédérales ont institué des chargés de la protection de la protection des données à la suite du vote du Privacy Act de 1974. Ces services typiquement se focalisent strictement sur la mise en œuvre du Privacy Act et ne jouent jamais de rôle dans la conduite d'une politique plus large de la protection des données. Dans les années 1990, le International Revenue Service et le ministère de la santé (Department of Health and Human Services) ont institué de petits services avec des fonctions plus larges. Le Congrès a institué le premier service de protection des données établi par la loi quand il a créé le ministère de la sécurité intérieure en 2002[34]. Cette fonction n'a pas d'indépendance. Le ministre désigne le chargé de la protection des données et la première personne désignée l'a été sur des critères politiques de sorte qu'elle soit dévouée au Président.

---

[34] *6 U.S.C. § 142.*

Des propositions de loi visent à donner à cette fonction plus d'autorité et une durée de mandat déterminée mais leurs chances d'aboutir sont très faibles. Reste maintenant à voir s'il est possible pratiquement ou politiquement de voir fonctionner un chargé de la protection des données à l'intérieur d'un ministère avec un degré réel d'indépendance.
Dans une loi de 2004, le Congrès a décidé que chaque agence fédérale devait désigner un responsable de la protection des données (Chief Privacy Officer) pour assumer la responsabilité principale de la protection des données et de la vie privée[35]. Cette disposition a été adoptée sans aucune audition ou débat parce qu'un sénateur l'a placée dans une loi de finances. Un membre de la Chambre des Représentants a déposé une proposition de loi pour abroger cette disposition avant même qu'elle soit définitive. S'il est vrai que cette obligation de prêter plus d'attention à la protection des données peut être opportune a un certain niveau, les responsables de la protection des données n'ont reçu aucun moyen pour accomplir la mission que la loi leur a confiée. Une autre disposition de la loi contraint les agences à engager des contrôleurs externes indépendants pour examiner leurs activités en matière de protection des données. La rumeur dit que cette disposition a été rédigée par un cabinet de consultants qui cherche à obtenir plus de contrats avec l'administration. Près d'un an après, presque rien n'a été fait pour faire entrer en application les prescriptions de cette loi.

3. Les études d'impact sur la protection des données (Privacy Impact Assessments – PIA)

En 2002, le Congrès a voté une loi imposant aux agences fédérales de conduire une étude d'impact sur la protection des données quand elles utilisent une nouvelle technologie informatique ou entreprennent de recueillir de nouvelles données[36]. Ce qui est exigé dans une étude d'impact n'est guère plus que ce qui est contenu dans les notices relatives à la protection des données déjà requises par le Privacy Act de 1974 sans aucune obligation pour les agences de procéder à une étude substantielle des conséquences sur le niveau de protection des données et de tenir compte des résultats des études qu'elles mènent. Bien que le système des études d'impact n'ait pas encore été évalué à ce jour, des éléments anecdotiques suggèrent que certaines agences ont réellement utilisé les études d'impact. Dans d'autres, le processus des études manque de substance, d'implication et de rôle clair dans le processus de prise de décision.

Secteur privé

4. La Federal Trade Commission

Les organismes évoqués ci-dessous concernent exclusivement les activités du gouvernement. La principale agence avec le plus de compétence sur le secteur privé est la Federal Trade Commission (FTC). La FTC a des responsabilités spécifiques dans l'application de plusieurs lois de protection des données. Dans certains cas, de nombreuses autres agences partagent ces responsabilités parce que le secteur économique concerné est soumis à de multiples régulateurs. Quand de multiples

[35] *5 U.S.C. § 552a note.*
[36] *44 U.S.C. § 3501 note.*

agences sont chargées du respect de la même loi, il est d'usage qu'elles émettent des réglementations identiques.
L'autre compétence de la FTC vient de sa capacité à poursuivre les actes ou pratiques déloyaux ou trompeurs[37]. C'est potentiellement un large pouvoir mais la compétence de la FTC sur le secteur privé n'est pas générale. D'importants secteurs de l'économie – banque, assurance, télécommunication – peuvent échapper à la compétence de la FTC. Échappe aussi à son pouvoir le large secteur des organismes sans but lucratif.
Si la FTC a émis certaines règles de protection des données. La nature de ses pouvoirs réglementaires rend difficile pour la Commission la promulgation de règles de ce type. La FTC a poursuivi quelques entreprises qui n'ont pas su se conformer à leurs propres politiques de protection des données parce qu'il est plus facile de faire une procédure pour pratique déloyale ou trompeuse contre une entreprise qui formalise sa politique de protection. Les entreprises ont ainsi appris qu'elles peuvent être en meilleure position si elles n'ont pas de politique de protection ou si elles ont une politique large, vague ou manquant de critères de mesure de son application.
Le pouvoir de la FTC a l'égard des pratiques déloyales ou trompeuses sert de support au contrôle de l'application de la protection des données, dont le programme Safe Harbor pour les entreprises qui veulent se conformer aux normes de l'Union européenne. La Commission fait que le programme semble être réellement appliqué, bien qu'elle soit si sélective dans le choix des dossiers dont elle se saisit qu'il est difficile de dire jusqu'à quel point son action est dissuasive. En outre, elle ne résout pas les problèmes individuels des consommateurs et peut n'offrir aucune aide réelle à ceux d'entre eux qui sont victimes d'une violation par une entreprise de sa politique de protection des données.

5. Les réponses des entreprises

Une récente réponse des entreprises aux préoccupations de protection des données a été l'institution de responsables de la protection des données (**Chief Privacy Officers** – CPO) dans beaucoup d'entreprises américaines. L'International Association of Privacy Professionals[38] (IAPP) indique qu'elle a plus de mille membres particuliers ou entreprises, et que beaucoup de ses membres sont CPOs dans de grandes entreprises. Le nombre et les fonctions réelles des CPOs d'entreprises n'est pas connu et il y a des indices que certains CPOs ont peu de pouvoir et de ressources, tandis que d'autres sont plus puissants. Certains fonctionnent essentiellement comme des contrôleurs de la conformité. Néanmoins, le fonctionnement d'une association structurée des professionnels de la protection des données est le signe que le mouvement des entreprises vers l'institution de CPOs a des racines solides. S'il est difficile d'évaluer ce mouvement, il est clair qu'il s'agit d'une activité substantielle. Quelles qu'en soient les raisons, beaucoup d'entreprises considèrent la protection des données comme un domaine qui requiert une attention et une coordination significatives. Alors que la législation américaine est encore occasionnelle, de grandes sociétés qui exercent de multiples métiers, et particulièrement celles qui opèrent à l'international trouvent que le simple suivi des règles applicables de protection des données est une tâche complexe. L'institution de

[37] *15 U.S.C. §57a(a)(1)(B).*
[38] *http://www.privacyassociation.org/.*

CPOs dans beaucoup de sociétés représente un effort sincère pour traiter les questions de protection des données. Le développement des CPOs a été encouragé en partie par une législation fédérale qui exige que chaque entité concernée ait un chargé de la protection des données. Dans les grandes institutions médicales, il est constant que ce soit un emploi à plein temps.
Un autre développement de la dernière décennie a été l'adoption de politiques de protection des données sur la plupart des sites web commerciaux. Ces politiques sont une réponse aux préoccupations des consommateurs, à la pression de l'administration et aux tentatives des entreprises d'éviter une réglementation d'origine législative. Par ailleurs, certaines législations imposent aux sites web, aux organismes de santé, aux banques et à d'autres d'avoir des politiques de correction. Si le contenu de ces politiques a été critiqué, l'augmentation de leur nombre est une évolution remarquable et, au moins dans certains cas, la réponse du marché aux préoccupations des consommateurs.

Les défenseurs de la protection des données

La communauté des défenseurs de la protection des données a cru en nombre et en importance durant la dernière décennie. Les associations leaders ayant une activité forte dans ce domaine sont l'Electronic Privacy Information Center (EPIC), le Center for Democracy and Technology, le Privacy Rights Clearinghouse, l'Electronic Frontier Foundation, l'American Civil Liberties Union (ACLU), le Public Interest Research Group, le World Privacy Forum, le Privacy Activism, etc. Beaucoup d'autres associations dont les sujets de préoccupation principaux n'ont pas de lien direct avec la protection des données participent aussi occasionnellement à l'activisme de ce domaine.
Même si les associations de défense de la protection des données ne jouent pas de rôle officiel dans aucun des mécanismes destinés à assumer le respect de la protection des données, il n'en ont pas moins d'importance. Ces associations détectent et rendent publics les problèmes concernant la protection des données et ils contribuent à entretenir cette culture des scandales de la protection des données qui tendent à diriger le cours des événements aux États-Unis. Ces efforts auront quelquefois un impact sur l'ordre du jour législatif à court terme mais ils ne contribuent pas nécessairement à prendre en compte ou à atteindre des objectifs plus larges et de stratégie à long terme.
Certaines associations sont des lobbyistes actifs pour faire passer des textes législatifs, en particulier en Californie et au niveau fédéral. D'autres aussi cherchent à utiliser la FTC pour faire avancer la cause de la protection des données. Dans plusieurs affaires récentes, la FTC a engagé des actions visant au respect de la protection des données, à la suite du dépôt d'une plainte, par une association, contre des pratiques d'entreprises. Pour des raisons qui ont été évoquées plus haut, les actions de la FTC laissent beaucoup à désirer mais il s'est avéré que les associations sont ravies qu'une réponse soit donnée à leurs plaintes.
Le monde des affaires tend à surestimer l'importance des associations dans le schéma général de l'élaboration et de l'application de la politique de protection des données. Les associations sont plus efficaces pour attirer l'attention du Congrès sur une question de protection des données. Toutefois, les lobbys des entreprises le sont plus pour obtenir des résultats quant au contenu même de la législation fédérale dans

ce domaine. Ce modèle va probablement se perpétuer tant qu'il n'y a pas de changement de majorité au Congrès et à la Maison Blanche. Néanmoins les associations se font entendre et ont parfois obtenu des compromis qui améliorent la protection des données.

Comme beaucoup d'autres choses dans la loi et la politique américaine de protection des données sont extrêmement variables dans leur forme, leur positionnement et leurs fonctions. Les administrations qui ont des responsabilités dans ce domaine ont toujours d'autres fonctions et il est constant que la protection des données soit pour elles, au mieux, une activité secondaire. Les structures émanant des entreprises sont difficiles à juger mais beaucoup d'événements de la dernière décennie tendent à montrer leur rôle positif. Une des raisons qui expliquent la faveur des réponses structurelles est qu'il peut être plus facile d'offrir des réformes procédurales que des restrictions substantielles aux fonctions des traitements de données. Les activités de la protection des données continuent à jouer un rôle majeur pour attirer l'attention sur les problèmes de la protection des données et aider à mettre ces sujets à l'ordre du jour législatif.

Conclusions

Au début de cette étude, deux visions nettement différentes de l'approche américaine étaient proposées. Beaucoup de jugements médians, en particulier au sujet de lois ou d'activités spécifiques, sont aussi possibles. Il n'y a pas de doute cependant que le cadre américain de régulation de la protection des données comporte de très grandes failles, défauts et faiblesses.
Seule une poignée de lois prennent complètement en compte tous les éléments des pratiques de l'information loyale et pourraient être valablement qualifiées d'adéquates au regard de la directive européenne de protection des données.

Les lois américaines contrôlent rarement les transferts de données personnelles et peu d'entre elles traitent expressément le cas où les données soumises à une réglementation seraient transférées dans un lieu relevant d'une réglementation plus faible. Une autre très grande faille est le manque de transparence. En particulier, le recueil, la conservation, l'usage et la diffusion de données personnelles par les entreprises se font souvent sans la moindre information des consommateurs. Des pans entiers des activités des traitements de données sont ignorés du public américain en raison de ce manque de transparence. Beaucoup de sociétés ne veulent pas dire aux consommateurs quelle quantité de données personnelles est recueillie de manière courante et comment ces données dont utilisées ou diffusées.

Deux sujets d'actualité différents donnent une illustration des dynamiques politiciennes et politiques de la protection des données. Le développement du vol d'identité a été une source majeure de législation. Á cause du vol d'identité, le public est maintenant parfaitement averti que le mauvais usage des données personnelles peut causer directement des dommages significatifs. Les défenseurs de la protection des données ont une réponse claire à l'argument des entreprises selon lequel les

consommateurs ne subissent pas de dommages du fait d'un large partage des données personnelles.

L'étalage continuel des coûts et conséquences du vol d'identité a poussé le gouvernement fédéral et beaucoup d'états à adopter des dispositions législatives ajoutant des sanctions pénales, étendant la compétence des tribunaux, fournissant de l'assistance aux victimes, créant de nouvelles garanties ou rendant obligatoire des mesures de sécurité. D'autres lois limitent le recueil et l'usage de données personnelles par des catégories spécifiques de données ou de responsables publics ou privés de traitement. Les parlements américains ont adopté beaucoup de lois en réponse au vol d'identité, ces efforts ne sont pas assez approfondis, ont peu dissuadé les délinquants et n'ont que peu amélioré le niveau général de protection des données. Certaines lois ont permis plus facilement aux victimes de faire face aux conséquences d'un vol d'identité et à l'administration de poursuivre les auteurs des infractions mais la publicité et la difficulté du vol d'identité ont dirigé l'attention vers des réponses secondaires loin de problèmes prioritaires de protection des données.

Cependant, la révélation en 2005 que ChoicePoint, un acteur majeur du commerce des données, avait une faille de sécurité qui avait exposé des données personnelles à des organisations criminelles de vol d'identité a accéléré de manière décisive les tentatives de législation. Plus d'états ont adopté des lois imposant aux entreprises d'informer les personnes concernées d'une violation de la sécurité de leurs données et une législation fédérale de préemption est actuellement en instance au Congrès et à une bonne chance d'être adoptée. Une législation fédérale cherchant à réglementer l'activité des marchants de données est aussi en instance quoique beaucoup d'observateurs aient des doutes sur son aboutissement.

Si l'on fait abstraction du résultat de ces travaux législatifs, ce scandale a été l'étincelle qui a transformé le débat sur le vol d'identité. Sa publicité a conduit à de nouvelles et plus larges propositions de réglementation du commerce des données, ce qui n'était pas du tout envisagé précédemment.

Cette affaire souligne l'importance de la publicité négative comme un levier dans le processus politique américain. Si une réponse législative émerge, ce sera sûrement une autre loi de protection des données réglementant un secteur particulier d'une manière différente des autres secteurs et qui continuera à laisser de nombreux traitements de données à l'écart de toute réglementation.

Le second exemple de question d'actualité est dans le domaine technologique. Une réponse américaine à la technique de l'identification par fréquence radio (RFID) est encore embryonnaire. Les conséquences des RFID pour la protection des données attirent une attention croissante de la part de l'industrie, des décideurs politiques, des défenseurs de la protection des données et des parlementaires. La FTC a organisé un colloque en 2004, la Californie a envisagé mais n'a pas adopté une législation définissant des normes pour l'usage des RFID dans les produits de consommation. Une récente loi fédérale a demandé une étude de l'usage des RFID les industriels de l'automobile. Des associations ont appelé au boycott de sociétés utilisant des puces RFID. Plusieurs ouvrages sur la technologie RFID et le problème qu'elle pose ont été

récemment publiés. Les normes de l'industrie (aussi bien aux États-Unis qu'ailleurs dans le monde) définies pour cette technologie ont prêté une certaine attention aux problèmes de protection de données.

Cet intérêt précoce pour ces problèmes dans le débat sur les RFID est relativement inhabituel aux États-Unis. Par contraste, le secteur du commerce des données s'est développé dans les deux dernières décennies sans aucune attention du public, des décideurs politiques ou du législateur. Le fait qu'il y ait un débat international sur cette technologie a pu aider à mettre la protection des données dans celui qui est mené aux États-Unis.
Il n'est pas possible cependant de prédire comment ou même si les États-Unis répondront finalement à ces questions. L'industrie apparaît fermement opposée à une législation mais cette position pourrait changer si un État réussit à adopter une loi. L'industrie pourrait alors chercher à obtenir une loi fédérale qui préempte l'action des États au motif que cette technologie requiert une seule norme nationale. Les préoccupations de l'opinion publique pourraient croître et contraindre à de meilleures réponses du marché ou à une solution politique. Toutefois, les préoccupations de l'opinion à l'égard de nouvelles technologies se sont, dans le passé, parfois, évanouies avec le temps. Quand l'identification de l'appelant a été introduite par les téléphones, elle a provoqué une opposition considérable. Avec le temps, cependant, cette technologie a été acceptée avec de modestes aménagements pour ceux qui craignent pour leur vie privée. L'usage des RFID pour les péages d'autoroute n'a suscité presque aucune controverse de ce point de vue.

Jusqu'à maintenant, il manque à la technologie des RFID le scandale souvent nécessaire pour déclencher le processus législatif américain. Certains usages sur des produits de consommation ont suscité opposition et publicité mais par jusqu'au point nécessaire pour surmonter la résistance de l'industrie à une législation et l'inertie du processus législatif. La réponse de l'industrie aux préoccupations exprimées par des défenseurs de la protection des données peut être suffisante pour apaiser les peurs de l'opinion publique. Les RFID restent une technologie qui, sur le plan de la protection des données, peut avoir différents résultats.

Sous bien des aspects, l'approche américaine de la protection des données est identique à celle suivie sur beaucoup d'autres questions politiques importantes aux États-Unis. Le système politique américain construit les lois et les institutions à travers un cycle de laisser-faire, changements progressifs et explosions occasionnelles d'action et d'innovation. Cette approche produit souvent des faiblesses et des failles. De larges évaluations et révisions des politiques ne sont conduites qu'occasionnellement et quand elles ont lieu, leurs résultats sont souvent ignorés. En 1977 une commission d'études sur la protection des données personnelles avait produit un rapport complet mais le Congrès n'a repris qu'une petite partie de ses recommandations législatives.

Les pressions rhétoriques et politiques pour des réponses données par le marché aux questions de choix de politique ou aux demandes des consommateurs ne sont pas limitées au domaine de la protection des données. Pas plus que l'importance de l'attention donnée par les médias aux scandales. De plus la législation américaine est souvent votée sans grand souci de ses conséquences internationales.

Il est difficile de suggérer que ces modèles devraient probablement évoluer à l'avenir dans le domaine de la protection des données. Certes, il y a de ci de là (en dehors de la communauté des défenseurs de la protection des données) la reconnaissance qu'une pléthore de lois de protection spécifiques et contradictoires crée des problèmes et des coûts de plus en plus élevés pour les entreprises. En plus, les pressions internationales dans ce domaine ont peu à peu accru l'attention pour le courant d'intérêt de la protection des données, les avantages de règles plus uniformes et le coût de régimes disparates de protection. Une des réponses à ces préoccupations de la part de la communauté d'affaires a été d'apporter quelque soutien au développement de règles internationales de protection des données pas aussi rigoureuses que celles figurant dans la directive européenne.

Néanmoins il est difficile de suggérer qu'il va probablement y avoir un large soutien pour une approche plus cohérente ou générale de la protection des données dans un futur proche. La structure législative fédérale rend difficile de voter des lois avec un champ étendu qui traverse les frontières sectorielles traditionnelles et les centres de pouvoir politique. En outre, il faudra beaucoup plus de temps et d'efforts avant que le besoin de donner une réponse aux questions de protection des données se répande à travers la communauté d'affaires américaine. Si l'intérêt de l'opinion publique pour la protection des données venait à diminuer, il est probable que cette communauté d'affaires démantèlerait tranquillement beaucoup d'efforts faits par elle dans ce domaine.

Les sujets qui vont continuer à focaliser l'attention de l'opinion publique et du législateur sur la protection des données et qui pourraient en fin de compte produire un changement dans l'approche américaine comprennent le vol d'identité, le « phishing » et d'autres activités criminelles sur Internet, les litiges relatifs à l'utilisation des données et les mesures anti-terrorisme. Si certaines actions anti-terrorisme ont des implications négatives pour la protection des données, le Congrès et les administrations ont aussi répondu en partie aux préoccupations relatives à la protection des données. Il reste possible que des pressions pour permettre plus d'intrusions dans la vie privée soient accompagnées dans le futur, pour les contrebalancer, par des mesures augmentant ou garantissant la protection des données d'autre manière. C'est ainsi qu'a été créé le premier organe fédéral officiel de protection des données, au sein du ministère de sécurité intérieure. De même, l'examen par le Congrès des actions en matière de sécurité aérienne du service de la sécurité des transports au sein du ministère de la sécurité intérieure a été fortement centré sur le besoin de garantir la protection des données dans le processus de contrôle des passagers.

Les limites constitutionnelles de l'action du pouvoir exécutif continuent d'être un aspect important des débats en cours sur la sécurité nationale. Les mesures

législatives et administratives surgissent souvent à la limite de ce qui est constitutionnellement possible et les cours servent fréquemment d'arbitres. Une évolution marquante résultant de la guerre contre le terrorisme est l'affaiblissement des distinctions traditionnelles entre les activités de l'État et du secteur public. De manière croissante, des fonctions de traitement de l'information qui seraient soumises à une réglementation si elles étaient conduites par des agences fédérales font l'objet de contrats passés avec des entreprises privées non soumises à réglementation. C'est un domaine où l'application au coup par coup de la législation sur la protection des données produit une différence significative. La loi qui s'applique au Gouvernement fédéral peut être contournée en louant les services du secteur privé pour faire du traitement de données.

Peut-être que le plus grand défaut de l'approche américaine de la protection des données est l'absence d'une agence fédérale de protection des données. Chaque fois qu'une question de protection des données surgit – souvent soulevée par la couverture médiatique d'un vol d'identité, de failles de sécurité ou d'usage déloyal d'informations personnelles par des entreprises ou par l'administration – l'administration typiquement répond comme si elle était confrontée à ces questions pour la première fois. Sans une source permanente de conseil sur la politique à mener, les décideurs du Gouvernement et du Congrès ont tendance à réinventer la roue à chaque fois. Alors que progresse lentement la reconnaissance des pratiques de l'information légale comme fondement d'une politique de la protection des données personnelles, chaque initiative pour mener une politique dans ce domaine tend à partir d'une page blanche. C'est une des raisons pour lesquelles les réglementations de la protection des données varient tant. En plus, la Federal Trade Commission et les groupements professionnels redéfinissent souvent les principes de l'information légale et utilisent ce label pour promouvoir des politiques qui ne sont pas conformes aux normes internationales. Quand une législation aboutit, elle tend à être caractérisée par un champ aux limites étroites, des possibilités réduites d'en assurer le respect et des règles de fond qui sont à la fois faibles et divergentes.

Une agence fédérale de protection des données indépendante pourrait aider à remédier à ces défauts. Elle pourrait fournir expertise, contrôle, assistance et une parole cohérente dans les débats sur la protection des données. En 1992, Spiros Simitis décrivait l'approche américaine de la protection des données comme « une régulation manifestement erratique, pleine de contradictions, caractérisée par un choix des sujets laissé au hasard et totalement déséquilibré »[39]. En 1989, le professeur David Flaherty observait : « Les États-Unis s'occupent de la protection des données différemment des autres pays et, globalement, moins bien, à cause de l'absence d'une agence de contrôle »[40]. Ces deux commentaires, pour ne pas être récents, décrivent encore correctement l'approche américaine de la protection des données. Il y a peu de raisons de s'attendre à un changement significatif d'approche dans un futur proche.

---

[39] *Spiros Simitis,* New Trends in National and International Data Protection Law, *in* Recent Developments in Data Privacy Law *22 (J. Dumortier ed. 1992).*

[40] *David Flaherty,* Protecting Privacy in Surveillance Societies *305 (1989).*

Mme. Suzanne INNES-STUBB
Avocate, White and Case LLP, Bruxelles

Les entreprises multinationales sont confrontées à plusieurs problèmes lorsqu'elles tentent de se mettre en conformité avec les lois applicables en matière de protection des données à caractère personnel. Il s'agit la plupart du temps de problèmes d'incohérence : soit une divergence entre différentes lois qui leur sont applicables ; soit des lois qui ne reflètent pas la réalité de l'informatique au sein d'une multinationale. Pour les multinationales d'origine américaine ou d'origine européenne mais ayant des filiales aux États-Unis, les entraves au bon respect de la loi sont particulièrement importantes.

Dans cette présentation, nous traiterons les trois problématiques qui semblent le plus souvent préoccuper ces multinationales : (1) les divergences de type juridique non seulement entre les États-Unis et l'Union Européenne, mais aussi en leur sein ; (2) le transfert de données hors de l'Union Européenne et les solutions législatives proposées à cette problématique qui ne reflètent pas toujours la réalité de l'informatique au sein des entreprises multinationales ; et (3) l'introduction peu systématique aux États-Unis de lois qui imposent une obligation d'informer les personnes dont les données ont été divulguées de manière illégale.

1. Les divergences juridiques

Les divergences transatlantiques

Il existe plusieurs exemples de différences juridiques entre l'Union Européenne et les États-Unis dans le domaine de la protection des données privées. Il est souvent fait référence au fait qu'en Europe, la législation est d'application **générale**[1] alors qu'aux États-Unis elle s'applique plutôt au niveau **sectoriel**. Mais les exemples décrits ci-dessous illustrent encore davantage les problèmes rencontrés par les groupes multinationaux qui cherchent une solution globale pour l'informatique :

- les données financières, qui sont parmi les mieux protégées aux États-Unis, n'ont même pas le statut de « données sensibles » en Europe ;

- les différences législatives en ce qui concerne le traitement des communications à des fins de prospection directe : le consentement préalable (opt-in) est d'application au sein de l'Union Européenne, alors que le système de « opt-out » s'applique aux États-Unis ;

---

[1] *La Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, J.O. L 281/31 du 23 novembre 1995; la Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques), J.O. L 201/37 du 31 juillet 2002.*

- l'absence dans la législation européenne d'une obligation d'informer les personnes dont les données ont été divulguées de manière illégale, alors qu'aux États-Unis, il faut tenir compte d'une multitude d'obligations à ce sujet;[1]

- la différence de traitement des alertes éthiques confidentielles : prescrites par la loi Sarbanes-Oxley aux États-Unis, de telles alertes anonymes ne sont pas en conformité avec certaines lois de l'informatique en Europe, sauf dans des circonstances très précises, comme nous l'avons récemment vu en France ;[2] et

- le traitement des transferts hors du pays dans lequel se trouve le responsable du traitement : l'Union Européenne interdit les transferts sauf si certaines conditions spécifiques sont remplies, tandis qu'une telle contrainte ne s'applique pas aux transferts hors des États-Unis.

Toutes ces divergences ne font que compliquer a vie du malheureux juriste d'entreprise qui essaie vainement d'expliquer la logique des lois sur l'informatique à sa direction.

Les divergences au sein de l'Union Européenne

Au sein de l'Union Européenne, les divergences de transposition au sein des différents États de la directive 95/46/CE compliquent inutilement la conformité aux lois nationales. Par exemple, dans plusieurs pays, les entreprises peuvent justifier le traitement des données du fait qu'il est nécessaire à la réalisation de leur intérêt légitime; dans d'autres pays, tels que la Pologne et la Finlande, cette légitimation est d'interprétation beaucoup plus stricte.

Dans quelques États membres (tels que la Pologne), le traitement des données des salariés se fonde **de préférence** sur le consentement, selon l'autorité polonaise de protection des données nationale. Dans d'autres pays, notamment en France, le consentement est **déconseillé** comme moyen de justifier le traitement de données des salariés.

Quant aux transferts des données vers un pays tiers à l'Union Européenne, le Royaume Uni interprète les justifications de tels transferts de manière beaucoup plus large que la plupart des autres pays.

En ce qui concerne la procédure administrative, les exceptions à l'obligation de notifier le traitement de données à l'autorité pertinente, ainsi que les formulaires de notification, varient énormément d'un pays à l'autre.

---

[1] *Toutefois, le groupe dit « de l'article 29 », qui rassemble les représentants de chaque autorité de protection des données nationale, aurait commencé à réfléchir à la possibilité d'introduire une telle obligation de notification dans l'Union Européenne, selon la Commission Européenne.*

[2] *Voir notamment le Document d'orientation adopté par la Commission nationale de l'informatique et des libertés le 10 novembre 2005 pour la mise en oeuvre de dispositifs d'alerte professionnelle conformes à la loi du 6 janvier 1978 modifiée en août 2004, relative à l'informatique, aux fichiers et aux libertés; http://www.cnil.fr/fileadmin/documents/La_CNIL/actualite/CNIL-docori-10112005.pdf .*

Enfin, le niveau de sanctions imposé par les autorités de protection des données et l'approche adoptée par ces autorités, sont parfois très différentes d'un État membre à l'autre. Si, en cas de défaut mineur de conformité, l'autorité britannique favorisera plutôt le **dialogue** avec l'entreprise concernée, en Espagne le risque d'une **amende** est beaucoup plus élevé. Il va de soi que l'approche britannique aura la préférence de la plupart des multinationales.

Les divergences aux Etats-Unis

Aux États-Unis, il existe quatre lois principales qui s'appliquent à des secteurs particuliers : la loi Gramm-Leach-Bliley dans le secteur financier;[1] la loi COPPA qui protège les enfants en ligne;[2] la loi HIPAA qui protège les données sur la santé ;[3] et la loi sur les agences qui enregistrent les données relatives au statut de crédit des consommateurs (le scoring).[4]

Il faut y ajouter quelques lois fédérales très spécifiques (comme une loi sur les données des conducteurs ou une autre sur la location de cassettes video), et encore une vingtaine d'autres qui obligent le responsable du traitement à informer la personne concernée lors de la divulgation illégale des données de celle-ci.

Vu la diversité des lois applicables aux États-Unis, il est facile de comprendre pourquoi le Senior Vice President et General Counsel de Microsoft, Brad SMITH, a fait part le 3 novembre 2005 de son souhait de voir une approche législative plus cohérente se développer au niveau fédéral aux États-Unis.

2. Le transfert de données hors de l'Union Européenne

Mais la problématique la plus grave pour les multinationales qui sont actives tant en Europe qu'aux États-Unis reste le transfert de données hors de l'Union Européenne.

La règle de base est claire : en vertu de l'article 25 de la directive 95/46/CE, le transfert de données vers un pays tiers à l'Union Européenne ne peut avoir lieu que si le pays tiers assure un niveau de protection adéquat. Les transferts vers la Suisse, le Canada (dans quelques secteurs), l'Argentine, Guernesey et l'Île de Man (toutes ces petites îles si importantes pour le secteur financier) ne sont possibles que par le biais de décisions dites « d'adéquation » prises de la Commission européenne.

Quant aux avantages et inconvénients (du point de vue des multinationales) des autres « solutions » éventuelles pour parer à cette problématique, telles que les dérogations, le *Safe Harbor*, les clauses contractuelles types et les règles internes d'entreprises, force est de constater que les entreprises multinationales sont souvent obligées de mettre en place une combinaison de ces méthodes, selon les données et les juridictions en cause.

---

[1] La loi Gramm-Leach-Bliley, dont les articles sur la protection des données privées se trouvent à 15 U.S.C. sections 6801 et seq.

[2] *COPPA (Children's Online Privacy Protection Act): 15 U.S.C. sections 6501 et seq.*

[3] *HIPAA (Health Insurance Portability and Accountability Act): 42 U.S.C. sections 201 et seq.*

[4] *Fair Credit Reporting Act: 15 U.S.C. sections 1681 et seq.*

Les dérogations

Un transfert de données peut se faire si la personne concernée a donné son **consentement** indubitable au transfert ou si le transfert est **nécessaire**, par exemple, à l'exécution d'un **contrat** entre la personne concernée et le responsable du traitement (ou dans l'intérêt de la personne concernée), ou si le transfert est nécessaire à la sauvegarde d'un **intérêt public**, à la défense d'un **droit en justice** ou à **la sauvegarde de la vie** de la personne concernée. Enfin, un transfert au départ d'un registre public est également permis sous certaines conditions.[1]

Si les dérogations à une interdiction n'assurent pas une protection pour les données faisant l'objet d'un transfert hors de l'Union Européenne, elles constituent néanmoins une solution importante à la problématique du transfert. Il est d'habitude moins coûteux et plus facile pour une entreprise de justifier un transfert sur la base d'une de ces dérogations que de mettre en place un système compliqué de contrats ou de règles internes contraignantes, par exemple.

Toutefois, ces dérogations sont interprétées de manière très étroite -- trop étroite aux dires de beaucoup de multinationales -- par les autorités de protection des données. Par exemple, même les autorités de protection les plus pragmatiques, comme celle du Royaume Uni, estiment qu'une décision organisationnelle ou économique d'une multinationale de situer sa base de données du service des ressources humaines dans un pays hors de l'Union Européenne ne peut rendre **nécessaire** le transfert vers un tel pays des données concernant des salariés.

Toutefois, il est très difficile d'expliquer à la direction d'une multinationale pourquoi sa décision « économique » implique une protection moins efficace des données en cause. La multinationale met en place les mêmes protections techniques quelle que soit la localité de la base de données. Pour plusieurs entreprises, il n'est ni facile ni logique de garder toutes les données des salariés, et même de sa clientèle, en Europe. Ces groupes se voient donc obligés de mettre en place d'autres solutions plus coûteuses sans qu'il n'y ait vraiment de risque pour les salariés ou les clients concernés.

La possibilité d'obtenir le consentement de la personne concernée est un moyen attrayant de se mettre en conformité avec la loi. Comme le consentement est souvent nécessaire pour le traitement des données sensibles, l'entreprise peut obtenir le consentement de la personne concernée pour le transfert hors de l'Union Européenne en même temps. Au premier abord, le consentement semble représenter la solution idéale au transfert de données des salariés. Toutefois, la possibilité de se fonder sur cette dérogation est également limitée : tout d'abord, il s'agit d'une solution peu pratique pour un grand nombre de personnes ou en cas de relation indirecte avec la personne concernée ; ensuite, la plupart des autorités en Europe n'acceptent le consentement des salariés que si le salarié est en mesure de refuser ou de retirer son consentement sans préjudice, ce qui est difficile de démontrer en pratique.

---

[1] *Voir l'article 26.1 de la Directive 95/46/CE, ainsi que le document de travail du groupe de l'article 29 du 25 novembre 2005 :* Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995*, WP 114*.

***Le Safe Harbor* (la sphère de sécurité)**

Le *Safe Harbor* est un programme établi par le *Department of Commerce* aux États-Unis et approuvé par la Commission européenne. Toute entreprise établie aux États-Unis qui s'engage à adhérer aux sept principes du *Safe Harbor*, est autorisée à recevoir des données à caractère personnel des pays membres de l'Union Européenne.

Les sept principes sont les suivants:

1. *Notice* : l'obligation d'informer les personnes sur les données rassemblées et les finalités de traitement de ces données ;

2. *Choice* : la possibilité de s'opposer à un transfert vers des tiers ou à des fins différentes de celles précisées lorsque les données ont été rassemblées (le consentement explicite est demandé en cas de transfert des données sensibles vers des tiers ou à des fins différentes) ;

3. *Onward Transfer* : l'obligation d'appliquer les principes de *Notice* et de *Choice* avant de transmettre les données vers un tiers ;

4. *Access* : le droit d'accès aux données et le droit de corriger ou d'effacer les données inexactes, sauf si l'exercice de ces droits devait entraîner des coûts pour l'entreprise considérés comme disproportionnés par rapport aux risques encourus par l'individu ;

5. *Security* : la protection des données contre la perte, l'abus ou l'accès non-autorisés ;

6. *Data Integrity* : l'obligation de ne traiter que des données qui sont pertinentes, exactes, complètes et mises à jour, au regard des finalités prévues ; et

7. *Enforcement* : une mise en vigueur appropriée et rigoureuse.

Parmi les avantages du *Safe Harbor*, citons les points suivants : il est reconnu partout au sein de l'Union Européenne ; un citoyen européen doit en général intenter un procès contre l'entreprise importatrice aux États-Unis (ce qui est bien entendu un avantage pour l'entreprise américaine, même si ce n'est peut-être pas le cas pour le citoyen) ; et le *Safe Harbor* est plus flexible que les clauses contractuelles que nous traiterons plus bas.

Toutefois, il existe deux restrictions importantes : tout d'abord, le *Safe Harbor* ne s'applique pas aux transferts à partir de l'Union Européenne vers d'autres pays tiers que les États-Unis, ce qui signifie qu'il ne constitue qu'exceptionnellement la seule méthode pour justifier des transferts effectués par un groupe multinational ; ensuite, le *Safe Harbor* ne s'applique pas dans tous les secteurs. Il n'est pas valable pour les services financiers, par exemple.

D'ailleurs, plusieurs entreprises ont renoncé à leur intention d'adhérer au *Safe Harbor* en raison de son entrée en vigueur par la *Federal Trade Commission* ou le *Department of Transportation* aux États-Unis, qui pourraient éventuellement imposer des amendes beaucoup plus élevées que celles possibles dans l'Union Européenne. En outre, les entreprises adhérentes doivent se soumettre aux autorités européennes en ce qui concerne les données des salariés (les salariés peuvent pour leur part intenter des procès dans l'Union Européenne), ce qui est moins pratique pour l'entreprise importatrice aux États-Unis.
En dépit de tous ces inconvénients, le nombre d'adhérents au Safe Harbor augmente progressivement. Au 4 novembre 2005, ils étaient 816, une augmentation de 121 entreprises depuis le 5 avril 2005.[1]

Les clauses contractuelles types

Il existe deux modèles de clauses contractuelles types destinées à encadrer les transferts de données vers des **responsables** de traitement établis hors de l'Union Européenne : les clauses de juin 2001, proposées par la Commission européenne ; et celles de décembre 2004 développées par une coalition d'associations professionnelles, menée par la Chambre de Commerce Internationale (« CCI »). La Commission européenne a approuvé un modèle de clauses contractuelles types pour les transferts de données vers des **sous-traitants** en décembre 2001.

L'avantage principal des clauses contractuelles types est la sécurité juridique à long terme qui en découle. De plus, ces clauses sont souvent conseillées pour les données des salariés. D'ailleurs, en adoptant les clauses CCI, les inconvénients des clauses de la Commission (telles que la responsabilité conjointe et illimitée, par exemple) peuvent être évités.

Toutefois, les clauses sont difficiles à mettre en oeuvre pour un groupe multinational composé de centaines d'entreprises dispersées à travers le monde. La gestion du réseau de contrats prend beaucoup du temps, surtout au cas où le groupe achèterait une nouvelle entreprise ou transférerait les données pour une nouvelle finalité, ce qui exigerait la modification des contrats. D'ailleurs, les clauses ne sont pas adaptées pour des succursales sans personnalité juridique. De plus, les clauses « CCI », qui sont les plus flexibles, donnent davantage de pouvoir aux autorités nationales européennes pour interdire ou suspendre les transferts, notamment si l'exportateur de données refuse de faire valoir le contrat à l'encontre de l'importateur dans un délai d'un mois.

Les règles internes d'entreprises («BCRs»)

Si les méthodes décrites ci-dessus semblent susciter de nombreux problèmes, la perspective de développer des règles internes d'entreprises (autrement dit les «Binding Corporate Rules » ou « BCRs ») devrait améliorer la situation des

[1] *La Commission Européenne, à l'occasion d'un « privacy workshop » qui s'est tenu le 7 décembre à Washington, D.C., a souligné sa préférence pour le* Safe Harbor *pour des transferts vers les États-Unis – une position qui contraste avec les doutes jetés sur l'efficacité du* Safe Harbor *par la Commission dans des années passées. Cette nouvelle position devrait encourager de nouveaux adhérents. Au 22 décembre 2005, le* Safe Harbor *comptait 846 membres.*

multinationales. Les BCRs se composent, selon la CNIL, d'« un ensemble de règles relatives à la protection des données personnelles élaborées par l'organisme du responsable de traitement, le plus souvent une société multinationale, dont le respect est obligatoire pour chacune des entités membres du groupe. »[1]

Quels sont les avantages des BCRs ? Les BCRs peuvent encadrer les transferts hors de l'Union Européenne au sein du groupe (mais pas en dehors du groupe). Elles sont plus flexibles que les contrats types, même si en pratique elles doivent inclure une majorité des éléments qui se trouvent dans les clauses types. Et, ce qui est le plus important, elles reflètent mieux l'informatique au sein d'un groupe multinational parce qu'elles sont développées pour et par le groupe lui-même.

Toutefois, les BCRs doivent être approuvées par l'autorité de protection des données de chaque pays exportateur dans l'Union Européenne – un inconvénient majeur. Malgré une nouvelle procédure rationalisée introduite au mois d'avril 2005 et selon laquelle une autorité nationale coordonne la procédure d'autorisation, certaines autorités nationales se réservent néanmoins le droit d'imposer certaines formalités administratives au niveau national.[2] Tant que ces obstacles nationaux persistent, et jusqu'à ce que les dix premières entreprises aient éprouvé cette méthode, il est difficile d'estimer le temps et les ressources financières dont il faudra disposer pour obtenir toutes les autorisations nécessaires. Par conséquent, les BCRs représentent actuellement un pas dans l'inconnu pour la plupart des entreprises.

3. L'obligation d'informer les personnes dont les données ont été divulguées de manière illégale aux États-Unis

Si le transfert de données hors de l'Union Européenne représente le problème majeur aux yeux des entreprises européennes, les entreprises américaines quant à elles sont davantage concernées par une loi californienne de 2003, une « Notification Law », qui oblige le responsable du traitement à informer la personne concernée dès que les données de celle-ci sont divulguées à une personne non-autorisée.[3]

Á la suite de cette loi, plusieurs entreprises ont informé des milliers de gens que leurs données personnelles avaient été divulguées de manière illégale. Citons le cas de ChoicePoint, où il s'agissait des données de 145.000 personnes, de Lexis Nexis (32.000 personnes) et encore de la Bank of America (plus d'un million de personnes).

Au moins vingt États ont actuellement des lois plus ou moins semblables, même si l'obligation d'information est induite par des circonstances légèrement différentes : en Californie, par exemple, c'est la divulgation de données vers une personne non-autorisée qui déclenche l'obligation de notification ; en Delaware, par contre, c'est l'abus probable de données. En outre, la loi californienne prévoit un droit d'action

---

[1] *Voir* Transferts de données à caractère personnel vers des pays non membres de l'Union européenne, *CNIL, octobre 2005, page 21.*

[2] *General Electric a annoncé le 15 décembre 2005 avoir réussi à faire approuver ses BCRs par l'autorité de protection des données au Royaume Uni, suivant la nouvelle procédure de coordination, mais la compagnie attend encore les autorisations des autres autorités pertinentes.*

[3] Voir Cal. Civil Code sections 1798.29, 1798.82, 1798.84. ou Calif. S.B. 1386 (2002-2003).

privée : d'autres lois ne le prévoient pas. Pour couronner le tout, plusieurs propositions de loi ont été également introduites au niveau fédéral.

Pour les entreprises aux États-Unis, il existe donc une situation d'incertitude juridique. Mais il est clair que la publicité négative liée à l'obligation d'informer les personnes concernées est la méthode la plus efficace pour augmenter le niveau de protection des données personnelles. C'est d'ailleurs grâce à cette loi californienne que les entreprises américaines ont commencé à prendre conscience de l'importance de la protection des données personnelles.

En conclusion, il est clair que le manque de convergence juridique dans le domaine de la protection des données à caractère personnel entrave le respect actuel de la loi, surtout au sein de l'Union Européenne, où il est presque impossible pour des multinationales d'être en conformité avec toutes les lois applicables.

Pour augmenter le niveau de conformité (ce qui est aussi bien dans l'intérêt des citoyens que dans celui des entreprises), il faudrait :

- soit une véritable **harmonisation** de la loi, soit une **reconnaissance mutuelle** au sein de l'Union Européenne, afin de faciliter la mise en conformité et la rendre moins coûteuse ;

- une **rationalisation** de la législation pour cibler les risques les plus graves (tels que les secteurs qui traitent les données financières ou les données sur la santé) ;

- une législation qui reconnaisse **la réalité de la pratique** de l'informatique au sein des multinationales (par exemple, les bases de données globales) ;

- une procédure administrative **moins lourde** (surtout en ce qui concerne l'obligation de notification et l'autorisation des BCRs) ; et

- une mise en vigueur plus efficace. Toutefois, je souligne qu'une obligation d'information de type « Loi Californienne » ne pourrait être considérée en Europe que si une vraie harmonisation et une vraie rationalisation de la loi actuelle étaient achevées. Dans le cas contraire, le fardeau qu'auraient à porter les multinationales ne ferait qu'entraver davantage le commerce européen.

4. Les continents vierges

M. Valeri VALERIEVICH FEDOROV
Professeur de droit constitutionnel, Directeur du centre de conjecture, Russie

M. Yves DOLAIS
Vice Président de l'Université d'Angers, Chargé de cours de droit chinois à l'Institut de Droit Comparé de Paris II

M. Yves DOLAIS
Vice Président de l'Université d'Angers,
Chargé de cours de droit chinois à l'Institut de Droit Comparé de Paris II

Internet en Chine : l'Intranet le plus vaste du monde ?

« La Chine va-t-elle devenir le plus grand Intranet du monde ? »[1]

Deux illustrations parmi bien d'autres :
- Au moment du décès du Pape Jean Paul II, toute référence à son décès avait été bloquée pendant quelques jours en Chine. C'est par leur téléphone mobile que les chinois se transmettaient l'information.
- Les adresses électroniques, du fournisseur d'accès chinois sina.com, fournies par de nombreux étudiants chinois rencontrés lors du Salon de l'Education en novembre 2004 en Chine par les universités françaises se sont avérées inaccessibles de France.

La question peut paraître excessive, mais elle est sérieuse. La Chine pourrait bien devenir le plus grand Intranet au monde, c'est-à-dire un espace clos où les internautes peuvent travailler, collaborer, échanger et créer de la valeur ajoutée en toute sécurité.

L'arrivée d'Internet en Chine avait, il y a quelques années, fait naître l'espoir d'un cheval de Troie favorisant la liberté d'opinion et d'expression et l'émergence d'un débat démocratique. Hélas, aujourd'hui, force est de reconnaître que les autorités chinoises ont pris le contrôle d'Internet.

---

[1] C'est ainsi que titrait dans son éditorial de début mars 2005 , Jean de Chambure, rédacteur en chef de l'Atelier.

Á la crainte initiale d'être submergée par ce nouvel espace de liberté, l'incitant à établir une « Grande Muraille électronique », the « Great Firewall », la Chine est passée au début des années 2000 à une prise de conscience du potentiel que représente Internet pour en faire un « bouclier doré », un outil de plus en plus puissant et sophistiqué de contrôle et d'exploitation de l'information au service du développement économique du pays et non au service de la liberté d'expression. La Chine veut « exploiter le potentiel phénoménal d'Internet pour faire entrer le pays dans la mondialisation tout en supprimant simultanément son potentiel en matière de liberté d'expression ».
La Chine se classe désormais au deuxième rang derrière les États-Unis pour le nombre d'usagers de la toile avec plus de 100 millions d'internautes, mais le taux de pénétration d'Internet dans cette population de 1,3 milliard de personnes est encore faible, à seulement 8% des foyers. La Chine compte également 376 millions d'abonnés à des services de téléphonie mobile, record mondial.

La compréhension de l'approche dirigiste d'Internet en Chine doit être replacée dans ses dimensions culturelles et politiques. La société chinoise qui n'a jamais connu de régime démocratique est encore sous-tendue par les principes confucéens de soumission sociale confortés par près de 60 ans de régime communiste, mélangeant souvent comme le faisait Mao Zedong rhétorique communiste et tradition confucéenne. Cependant l'introduction en mars 2004 dans l'article 33 de la Constitution chinoise du principe de protection des droits de l'homme et la libéralisation fin 2003 des modalités du mariage et du divorce, supprimant l'obligation d'une attestation de l'employeur ou des autorités locales, marquent un progrès. Toutefois, si le droit à la vie privée recouvre une réalité croissante en Chine, la liberté d'expression tend à devenir de plus en plus une liberté surveillée dans la stratégie informatique chinoise.

La stratégie chinoise est à double orientation interne et internationale.

Sur le plan international, la Chine veut peser désormais sur le futur de la Toile, qui sera débattu au 2ème Sommet mondial sur la Société de l'Information organisé par l'ONU à Tunis du 16 au 18 novembre 2005, en remettant en cause la gouvernance actuelle de l'Internet au même titre que d'autres dictatures comme l'Iran, afin de mieux contrôler le web sur son propre territoire.

Sur le plan interne, le gouvernement chinois pratique une politique d'ouverture en encourageant l'implantation d'Internet (le ministre des Affaires étrangères a même participé à un chat chinois) tout en mettant en place progressivement une infrastructure très sophistiquée de contrôle, qui est confortée depuis le 11 septembre 2001 par le virage sécuritaire mondial.

Internet en Chine, c'est :
- Un outil sécurisé au service du développement économique
- Un outil d'information et de propagande au service du pouvoir
- Le réseau Internet le plus sophistiqué au monde en matière de contrôle
- Une répression accrue

- Une légalité très contestable

1. Un outil sécurisé au service du développement économique

La Chine a consacré d'importants moyens à l'équipement informatique du pays. « L'informatique régit le développement du pays, de la modernisation de son armée à la compétitivité de ses entreprises sur le plan mondial ». L'accès à Internet a explosé en Chine, passant de 8 millions d'internautes en 1999 à 59 millions en décembre 2002 et à plus de 100 millions en novembre 2005.

Le commerce électronique devrait atteindre 6,5 milliards de dollars en 2007. La loi sur les contrats du 1er octobre 1999 intègre désormais le commerce électronique. L'échange de données électroniques et les courriers électroniques sont définis comme étant des écrits (article 11) et depuis le 1er avril 2005, la reconnaissance juridique de la signature électronique permet de garantir la sécurité des échanges en ligne[1]. Les messages électroniques peuvent aussi servir en tant que moyens de preuve.

Le développement d'Internet favorise aussi la modernisation de l'administration et son accessibilité, ainsi qu'une meilleure connaissance et application de la réglementation chinoise contribuant à une plus grande effectivité du « gouvernement par la loi » selon l'expression de l'article 5 de la Constitution chinoise.

L'Administration d'État de la Presse et de la Publication et l'Administration d'État des Droits d'Auteur ont publié récemment plusieurs décrets appelant les autorités concernées à renforcer le contrôle contre le piratage sur Internet dans l'ensemble du pays. Il s'agit de l'opération la plus importante menée par la Chine en la matière. Avec la généralisation et le développement des techniques d'Internet, le téléchargement ouvre un accès aux produits audio-visuels et jeux illégaux sur le marché chinois. Le piratage sur Internet est donc devenu une grave menace pour les droits d'auteurs chinois et étrangers.

2. Un outil d'information et de propagande au service du pouvoir

Les forums de discussion (Lun Tan) sont devenus très populaires et sont principalement consacrés aux questions de consommation, d'éducation et d'emploi[2] mais ils sont souvent instrumentalisés, ainsi ceux sur la guerre en Irak[3] ou ceux relatifs au Japon lors de la polémique sur les manuels d'histoire au Japon et des manifestations anti-japonaises d'avril 2005.

3. Le réseau Internet le plus sophistiqué au monde en matière de contrôle

---

[1] En France par la loi du 13 mars 2000.

[2] Selon les chiffres publiés par le CNIIC (China Internet Network Information Center). La recherche d'informations politiques et internationales ne serait prioritaire.

[3] 900.000 messages le 4 avril 2004 sur le forum sur la guerre en Irak du portail Xinhuanet.com. Le gouvernement a aussi diffusé une version modifiée d'un rapport du Pentagone sur l'armée chinoise en juillet 2005.

Le Gouvernement chinois associe le fort développement de l'usage d'Internet avec un arsenal technique et juridique de contrôle et de répression fait de mesures de filtrage, de surveillance, d'autocensure et de sanctions.
Le filtrage, qui utilise les technologies d'interception des communications électroniques et de censure du Réseau les plus performantes acquises auprès de sociétés comme Cisco ou Thales, consiste soit à bloquer temporairement des sites (plusieurs dizaines de milliers), soit à bloquer la recherche de certains mots-clés sur les sites (plus de 40.000 selon certaines sources). Tous les ordinateurs des cybercafés sont équipés de logiciels de filtrage.
La surveillance, c'est l'armée des cybercenseurs, fonctionnaires dotés du pouvoir de gommer les pages d'un forum d'un coup de souris, de faire disparaître les courriels inappropriés, voire d'accumuler les preuves avant poursuites. Le chiffre de 20 000 à 50 000 cyberpoliciers rivés à l'écran 24 heures sur 24 et présents dans 700 villes a pu paraître exagéré jusqu'à ce que la municipalité de Pékin annonce à l'été 2005 qu'elle recherchait 4 000 diplômés de l'université pour en faire des cyberagents chargés d'éliminer «les informations malsaines» dans la seule capitale chinoise.
L'autocensure, celle des internautes d'abord et puis celle des webmestres, concerne toute la chaîne et est très encouragée par la réglementation. Mêmes les sociétés étrangères y sont soumises. Yahoo !, Google, Microsoft ont signé des engagements d'auto-censure. Yahoo ! a reconnu avoir communiqué à la police les mails et numéros de téléphone d'un journalisme chinois, Shi TAO, qui a été condamné en avril 2005 à dix ans de prison « pour avoir divulgué des secrets d'État à l'étranger », en l'occurrence le contenu d'un avis du service de propagande du PCC interdisant de couvrir le 15ème anniversaire du massacre de Tian An Men. Cette affaire qui a fait grand bruit soulève une polémique autour des enjeux économiques de ces sociétés en Chine.
Les sanctions qui vont de la fermeture d'un site à des peines de prison sont de plus en plus lourdes.

Après une brève période d'effervescence brouillonne, l'Internet chinois se retrouve soumis progressivement depuis 2000 à la même coupe réglée que la presse, quatrième pouvoir «à nouveau réduit au rôle de courroie transmission[1]», comme le regrette un journaliste pékinois. Seule l'information sanctionnée par le régime et par l'Agence d'État Chine nouvelle peut désormais s'afficher à l'écran, sous peine de s'exposer à des amendes dissuasives de 10 000 à 30 000 yuans par infraction (1 000 à 3 000 euros), à la suspension de leur compte, voire à la prison.

Les autorités chinoises ont réussi à dresser tout autour du pays une sorte de bouclier idéologique qui permet d'isoler l'Internet chinois du reste du monde. Dès le départ, le but était de limiter l'accès des Chinois aux informations gênantes pour le régime, qu'elles traitent de la démocratie ou de la répression.

La nouvelle réglementation, promulguée fin septembre 2005 par le gouvernement central, vise un autre objectif : il s'agit de limiter l'aptitude des Chinois à exprimer publiquement des opinions personnelles, notamment dans les forums de discussion et

[1] *Plusieurs gouvernements provinciaux chinois ont récemment demandé au gouvernement central d'interdire aux journaux nationaux la couverture des manifestations et évènements dans leurs provinces.*

sur les blogs, voire par courriel. «Après avoir canalisé l'information, il s'agit de bloquer le commentaire», résume un spécialiste chinois.

Le règlement du 25/09/2005

Ce nouveau règlement, promulgué par le Bureau de l'Information du Conseil des Affaires d'État et le Ministère de l'Industrie et de l'Information, concerne les responsables de sites Internet et des bloggers. Il harmonise les textes existants et énonce une liste de 11 interdictions dont deux nouvelles, l'évocation des grèves, émeutes et autres troubles sociaux qui agitent le pays, et l'organisation d'activités ou associations illégales via Internet. Les sanctions prévues seront la fermeture du site et une amende maximum de 30.000 yuans (3.000 euros).[1]

4. Une répression accrue

Reporters sans frontières rappelle que 62 personnes sont actuellement emprisonnées en Chine pour avoir diffusé des textes jugés « subversifs ».
Depuis l'adoption du règlement du 25 septembre 2005, les autorités, inquiètes devant la montée des mécontentements sociaux, multiplient les censures de sites Internet et de blogs traitant des manifestations sociales[2]. Beaucoup d'internautes ont en particulier informé sur les évènements de Taishi, ce village de non-droit du sud de la Chine (Guangdong) où les habitants se sont mobilisés contre la saisie de leurs terres à des fins de spéculation immobilière et contre la corruption du chef du village et où des journalistes et même un député chinois ont été tabassés par des milices.
Autre exemple : Shi XIAOYU, un internaute syndicaliste, a été arrêté le 20 octobre 2005 pour avoir mis en ligne des informations sur la répression policière violente contre des manifestations d'ouvriers sidérurgistes de Chongqing opposés à la corruption de certains dirigeants[3].

---

[1] Selon le quotidien chinois Beijing News (thebeijingnews.com), cité par RSF, le document mentionne onze interdictions à l'attention des éditeurs en ligne. Il est notamment prohibé de diffuser des informations qui :
- violent les principes de base de la Constitution chinoise ;
- mettent en danger la sécurité nationale, révèlent des secrets d'État, incitent à la subversion de l'État ou mettent en danger l'unité du pays ;
- portent atteinte à la réputation du pays ;
- développent la haine, le racisme et mettent en danger l'harmonie ethnique du pays ;
- violent les lois nationales sur la religion, ou promeuvent les sectes et les superstitions
- propagent des rumeurs, mettent en danger l'ordre et créent une instabilité sociale ;
- ont un caractère pornographique, violent, ou lié aux jeux de hasard ;
- diffament ou portent atteinte à la réputation des personnes ;
- incluent des informations illégales au regard de la loi ou des règlements administratifs.

Deux interdictions inédites ont été ajoutées à ces neuf règles :
- Il est interdit d'encourager les rassemblements illégaux, les grèves, les troubles à l'ordre public ;
- Il est interdit d'organiser des activités illégales ou de créer des associations illégales par le biais d'Internet.

[2] *Trois sites ont été fermés début octobre ; le Forum de Yannan, évoquant les troubles de Taishi, et deux sites mongols accusés de messages séparatistes pour avoir proposé une assistance juridique aux habitants de Mongolie intérieure en conflit avec l'État. Cf. Libération 5/10/2005.*

[3] *RSF 27/10/2005. Autre exemple : Wang YI, enseignant à l'université de Chengdu, intellectuel démocrate, a vu son blog fermé par l'hébergeur Tianya sur ordre du bureau de surveillance*

5. Une légalité très contestable

Tant les restrictions à la liberté d'expression que les sanctions pénales prises sont d'une légalité contestable au regard du droit chinois et des engagements internationaux de la Chine.

La liberté d'expression

L'article 35 de la Constitution de 1982 stipule que « les citoyens jouissent de la liberté d'expression, de la presse, de réunion, d'association, de défiler et de manifestation ». L'article 36 pose le principe de la liberté religieuse. L'article 40 garantit la liberté et le secret de la correspondance des citoyens.
L'ensemble de ces articles ont été confortés par l'introduction en mars 2004 du principe de protection des droits de l'homme dans l'article 33.
En outre, la Chine a signé mais pas encore ratifié le Pacte des Nations Unies relatif aux droits civils et politiques.
Mais la Constitution chinoise est plus une déclaration de principe, symbolique dont les articles sont rarement invoqués devant les tribunaux.
Facteur aggravant, aucun contrôle de constitutionnalité des lois et des règlements n'existe encore. Ce sujet est aujourd'hui débattu en Chine[1]. L'absence d'une hiérarchie des normes rigoureuse et les nombreuses initiatives réglementaires « sauvages » des collectivités territoriales rendent plus illusoire un réel respect des principes constitutionnels.

Les atteintes à la liberté d'expression

L'utilisation quasi systématique de l'article 105 du code pénal relatif au crime « d'incitation à la subversion contre l'État » comme fondement juridique des condamnations des internautes par les tribunaux chinois est révélatrice du mépris du pouvoir et des tribunaux pour la liberté d'expression et de la volonté de criminaliser celle-ci[2]. Les peines encourues peuvent aller de 2 à 12 ans d'emprisonnement pour subversion ou menace à la sécurité de l'État. Cependant les condamnations en demi-teinte sont fréquentes[3] ; elles sont révélatrices de l'embarras du pouvoir face au développement d'Internet.

---

d'Internet quelques jours après qu'il ait été nominé par une radio allemande dans un concours international de blogs sur la liberté d'expression. RSF 3/11/2005.

[1] Un journal chinois (Study Times du 11/04/2005), boite à idées du PCC, juge incomplète la protection des droits des citoyens et propose un système de contrôle de l'application de la Constitution et la création d'un organisme de contrôle de constitutionnalité des règlements.

[2] La Cour supérieure de l'Anhui a confirmé en appel le 14/10/2005 la condamnation à 5 ans de prison et 4 ans de privation de droits civiques de Zhanglin, coupable d'avoir accordé une interview à une radio étrangère, d'avoir publié des articles sur Internet, « contraires aux fondements de la Constitution » et « d'atteinte à la sécurité nationale ».

[3] Un internaute, Du Daobin, a été reconnu coupable « d'incitation à la subversion de l'État » le 11 juin 2004 par un tribunal du Hubei et condamné à 4 ans de résidence surveillée et déchu de ses droits civiques pendant deux ans, sentence confirmée en appel par la Cour supérieure du Hubei. Il avait été arrêté pour des articles en faveur de la démocratie. Son procès a duré 15 minutes, ni lui ni son avocat n'ont pu s'exprimer. Sa condamnation a été jugée par tous comme clémente au regard des peines habituelles et visait à apaiser les critiques soulevées en Chine et à l'étranger.

Une double conclusion peut être avancée :

Sur un plan interne, l'éventuelle libéralisation d'Internet est liée à une hypothétique réforme politique. La grande majorité des internautes chinois intègrent sans difficulté et sans sourciller les contraintes imposées. Certains observateurs, tel Human Rights in China (HRIC), estiment que la Chine mène un combat perdu d'avance puisque le grand public devient de plus en plus doué pour contourner les pare-feu gouvernementaux (HRIC – 23 juillet 2003). Le cybermilitantisme se développe malgré tout en Chine.
L'espoir demeure que la cyberrévolution finira par apporter à la Chine ce que les réformes économiques, engagées depuis plus de vingt ans, n'ont pas déclenché : l'éclosion d'une société civile, échappant au contrôle de l'État-Parti, à défaut de multipartisme. Optimisme ou utopie ? Le gouvernement chinois a publié le 19 octobre 2005 pour la première fois un livre blanc sur la démocratie où il réaffirme que « la direction du pays par le PCC est la garantie fondamentale pour que le peuple reste maître du pays et pour que le pays soit gouverné par la loi ».

Sur un plan international, le modèle chinois fait des émules (Vietnam, Cuba, Iran, Emirats Arabes Unis, etc..) et intéresse bien au-delà du cercle des régimes autoritaires. Est-ce la fin de la liberté totale ?

C. CONCLUSION DU COLLOQUE

Gouvernement mondial ou appropriation par le citoyen des outils de régulation ?

M. Dominique WOLTON
Directeur de recherche au CNRS

Je n'ai pas pu assister à l'ensemble des débats mais je peux dire pour avoir fait quand même beaucoup de débats depuis une vingtaine d'années sur les questions d'informatique, libertés et démocratie que celui-ci, je le dis sans faire de flagornerie, puisque la diplomatie n'est pas ma principale qualité, je l'ai trouvé extrêmement intéressant et évidemment surtout la dimension comparative : on ne dira jamais assez combien pour penser, on a besoin de comparer. Je dirais que le contexte chinois, le dernier qui nous a été présenté est quand même bien agréable. C'est-à-dire qu'il me permet d'illustrer ce que j'essaie de dire depuis trente ans, c'est qu'il n'y a aucun rapport entre la performance d'un système technique et la démocratie. Ce que les Chinois prouvent très bien : ils vont être capables de généraliser, y compris de faire des blogs, et de conserver un système policier. D'ailleurs je trouve que nous devrions élargir ce raisonnement : ce n'est pas parce que le capitalisme se développe en Chine qu'il y aura un jour de la démocratie en Chine. Le problème c'est que l'idéologie occidentale est assez courte et qu'elle a tendance à penser que plus on fait du commerce et plus la démocratie est au bout du chemin. Je ne vois pas au nom de quoi, hors de notre propre histoire qui a quand même mis trois siècles pour y arriver, il faille la généraliser. Au contraire, je trouve que le dernier exposé illustrait exactement l'ambiguïté permanente qu'il y a entre la confusion liée à la performance des systèmes d'information et la question de la démocratie.

Pour conclure, j'essaierai de développer quatre idées.

La première c'est qu'un système d'information, ce dont on parle aujourd'hui ici, c'est en général trois choses : **c'est naturellement de la technique, c'est de l'économie et c'est du social**. Et dans le social, il y a deux choses, le comportement des usagers et la volonté de régulation politique. Ce qui me frappe depuis – je travaille sur ces questions là depuis exactement trente ans –, c'est que dans cet ensemble de trois données, la technique, le marché et le social, je parle des sociétés démocratiques occidentales c'est globalement une adhésion quasiment passionnée à l'égard des progrès techniques et des possibilités du marché. Et par rapport à cela, la problématique de l'intérêt général dont la CNIL est un exemple extraordinaire, est très souvent à contre courant. On est quand même encore dans un imperium de l'idéologie technique, dans un imperium du marché, dans une fascination des usagers pour ce qu'ils peuvent faire sur les blogs et ailleurs.

Regardons simplement tout ce que l'on dit depuis un an sur le génie des blogs. Invraisemblable ! Après les chats, après les forums, hallucinant. Donc tous les six mois il y une nouveauté technique qui permet de montrer qu'on est dans une nouvelle étape de la démocratie parce que n'importe qui peut raconter sa vie sur un blog. Mais si tout le monde s'exprime, qui écoute ? Autrement dit, une fois que tout le monde aura raconté sa vie, il faudra bien qu'on se pose la question de savoir que ça n'intéresse en règle générale jamais les autres, c'est donc ce que j'appelle les « solitudes interactives » mais elles sont maintenant mondialisées. Les autorités indépendantes, ou les pouvoirs publics ou tous ceux qui sont garants de l'intérêt général sont hélas en position défensive pour l'instant. On a l'impression quand on veut réguler Internet ou quand on veut réguler l'espace des systèmes, on a l'impression d'être à contre-courant et d'être conservateur. Il y a une collusion entre l'idéologie technique et les valeurs de liberté.

Les principes de régulation sont faibles. Les technologies et les marchés s'additionnent et comme le disait très bien hier M. Gauthronet dans son exposé, il peut parfaitement y avoir individualisation à la fois des techniques et des marchés et augmentation des logiques de fichiers de contrôle. Mais le paradigme culturel dans lequel nous sommes est exactement l'inverse : on pense que plus c'est individualisé, plus c'est libre. Comment arriver, après quelle catastrophe, à quelles conditions historiques politiques, à faire basculer ce paradigme culturel qui identifie l'information et les libertés – plus d'informations et encore plus de libertés – et toute volonté de contrôler ces systèmes comme une atteinte à la liberté ? C'est évidemment l'expérience de la CNIL que je trouve extrêmement intéressante parce qu'elle essaie « avec ses petits poings » comme on dit, de réguler. Donc premier point : technologie + marché + fascination des usages l'emportent largement par rapport à toute volonté critique.

Deuxième idée que je voudrais développer : **la difficulté à faire prévaloir des valeurs sur l'intérêt des techniques ou sur la fascination des marchés vient du fait que la régulation est à chaque fois en porte-à-faux par rapport aux valeurs dominantes**. Je vais prendre deux exemples liés aux systèmes d'information. Si on prend les systèmes d'information au sens large, tels qu'ils existent dans la société, ce qui domine c'est le sentiment d'une abondance extraordinaire. L'information fut longtemps identifiée à la rareté ; depuis une cinquantaine d'années, l'information est liée à l'abondance. Du coup, pour tous les systèmes d'information auxquels nous pouvons accéder les uns les autres, le sentiment de liberté l'emporte, et, même si on admet aujourd'hui qu'il y a partout de la traçabilité, on dit en gros, « c'est pas grave, la traçabilité est moins grave, moins dangereuse que les avantages de libertés et d'abondance. » C'est ce deuxième paradigme culturel que je veux souligner : on ne croit pas que les inconvénients de traçabilité, soit pour les libertés privées, soit pour les libertés publiques, soient plus embêtants que les avantages de pouvoir faire soi-même un certain nombre de choses. Y compris ce que nous entendons du côté de l'école qui consiste à dire que grâce à un ordinateur, grâce à un réseau, des gamins et des gamines vont pouvoir enfin accéder à la connaissance, connaissance à laquelle ils refusent d'accéder grâce à leur professeur. Il y a partout cette idée, qu'en définitive, si quelqu'un fait quelque chose tout seul devant son clavier, il aura de la créativité, de l'intelligence, de la liberté, de

l'émancipation. Face à ce paradigme culturel – c'est quasiment une idéologie –, toute problématique de régulation est considérée comme conservatrice. On vous dit « quoi ? vous allez atteindre à cet immense mouvement qui est un mouvement vers l'émancipation, vers l'abondance ? » L'idéologie de la dérégulation est beaucoup plus forte que l'idéologie de la régulation. Donc le droit est, là, aperçu comme quelque chose de contraignant, malgré tous les dégâts de cybercriminalité que nous avons en exemple depuis une trentaine d'années. Autrement dit, la politique comme principe de régulation des systèmes d'information est toujours considérée comme quelque chose de conservateur et de réactionnaire ou d'antiprogrès.

Si l'on revient maintenant au problème d'idéologie sécuritaire, qui anime profondément les travaux de la CNIL, on retrouve la même ambiguïté mais à l'envers : l'idéologie sécuritaire cohabite *paradoxalement* avec l'idéologie de libertaire d'Internet. Pour une part, beaucoup adhèrent à l'idéologie libertaire, et pour une part, les mêmes acceptent que, finalement, il puisse y avoir des logiques sécuritaires pour garantir la démocratie.

L'idéologie sécuritaire va, si je puis dire, être admise indépendamment des atteintes à la liberté individuelle qu'elle peut produire. Du coup, la régulation politique se retrouve de nouveau à contre-pied, parce que finalement, dans le cas précédent, il s'agit de faire intervenir un principe d'intérêt général contre une idéologie de la liberté ; dans le cas de l'idéologie sécuritaire, il faut au contraire desserrer l'étau et réintroduire la liberté individuelle. Le principe politique se retrouve lui-même à contre-pied. Dans un cas d'idéologie libérale, on a du mal à faire prévaloir l'intérêt général, dans l'autre cas, quand l'idéologie sécuritaire domine, on a du mal à faire prévaloir un principe libéral. Mais dans les deux cas, c'est l'intérêt général qui est en cause et il se retrouve à chaque fois à contre-pied par rapport à l'idéologie du moment. Et quand hier après-midi je rappelais la phrase de La Boétie « attention à la servitude volontaire », c'est exactement ceci : les mêmes qui sont libertaires, sont d'autre part tout à fait prêts à accepter les méfaits d'une idéologie sécuritaire. Parce que le même homme qui, pour une part, veut la liberté individuelle, sera, au nom des intérêts de la sécurité, prêt à accepter un certain nombre d'atteintes les plus fondamentales aux libertés essentielles. L'exemple le plus patent, ce n'est pas la peine d'aller loin, c'est l'après 11 septembre aux États-Unis : le Patriot Act est quelque chose qui est inconcevable dans l'idéologie américaine libérale et cependant, il est parfaitement passé. Cela veut dire que dans les deux cas, qu'il s'agisse de l'idéologie de l'abondance ou de l'idéologie de la sécurité, l'intérêt général a toujours beaucoup de mal à se faire entendre parce qu'il est contradictoire et surtout d'une certaine manière et à chaque fois, en porte-à-faux. C'était ma deuxième idée.

La troisième, c'est de revenir à ce qui m'obsède depuis des années, une réflexion critique sur le statut de l'information. L'hypothèse est simple : si les gens ne comprennent pas la nécessité de réguler d'une part et le fait qu'il faille préserver des systèmes d'intérêt privé, il faut comprendre pourquoi ce mot de système d'information au sens large fascine autant dans la conscience occidentale. Il fascine, je crois, parce que, pendant des siècles, l'information se fit synonyme de liberté ou d'émancipation : liberté de conscience, liberté de parole, liberté de la

librairie, liberté d'opinion, liberté de la presse etc. Et toute la philosophie occidentale est une philosophie qui repose sur la liberté de l'information et de la communication. Tout ce qui était de l'ordre du contrôle ne relevait pas de la liberté d'information, mais de l'arbitraire. **Ce qui a changé en cinquante ans, c'est que les systèmes d'information portent à la fois la liberté et le contrôle**. Le mot «information » va aussi bien pour la liberté d'information au sens du XVIIIe, que pour les systèmes d'information au sens totalitaire, si l'on prenait l'exemple chinois aussi, puisque ce sont les mêmes systèmes techniques qui font les deux. Donc ce qui a changé, c'est la définition du mot « information ». Il peut simultanément, dans son ambiguïté, renvoyer aux grands concepts de libertés politiques, comme il peut renvoyer aussi à des systèmes totalitaires liés aux systèmes d'information. C'est parce qu'il y a aujourd'hui cet amalgame au sein des systèmes techniques du mot « information », que les systèmes d'information bénéficient globalement dans le monde d'une aussi grande appétence ou intérêt. Autrement dit, aujourd'hui le progrès technique réunit les deux sens de l'information : l'information à la fois liberté et l'information potentiellement contrôle.

Il faut, et notamment pour tout ce qui concerne les biométries, réduire au minimum les situations où on met des contrôles de type biométrique. Non seulement respecter la proportionnalité, mais aussi le pluralisme. Et si on veut qu'une réflexion critique naisse sur les systèmes d'information au titre de leur dimension de contrôle, il faut préserver dans la société d'*autres* formes de contrôle que les systèmes d'information : par exemple, du papier ou les contrôles humains. Autrement dit, éviter cette fascination rationalisée et technocratique qui consiste à croire que si on informatise tout, la société sera plus circulante, plus fluide. Pour que les réflexes critiques viennent plus vite, il faut maintenir des cultures politiques différentes. Autrement dit, il faut éviter que la logique système d'information englobe tous les systèmes de communication et d'information dans notre société. D'autre part, il faut toujours relier l'existence d'un système d'information « rationnel » aux questions, toujours les mêmes, de bon sens, pour qui ? pourquoi ? pour quelle finalité ? pour quel projet ? pour quelle réglementation ? pour quel système de valeurs ? autrement dit ne jamais accepter la performance d'un système d'information sans reposer les questions constantes de finalité. Refuser la segmentation au maximum, parce que, comme l'a très bien dit un des intervenants, plus il y a de segmentation et d'individualisation, moins il y a de responsables, parce que chacun des responsables fait du saucissonnage dans le domaine dans lequel il est. Donc on peut très bien arriver, au titre de l'individualisation ou au titre d'une société plus interactive, rappeler également que ce qui est à la base de tout système d'information, c'est la plupart du temps une logique économique, et que cette dimension économique, la plupart du temps, soit débouche sur une situation de commerce soit sur une dimension de contrôle d'une manière ou d'une autre, mais qu'elle n'a rien à voir avec une politique démocratique de l'information. Donc, trouver mille et une manière pour à chaque fois distinguer dans ce mot information et système d'information, ce qui relève d'une problématique économique ou technique de ce qui relève d'une problématique d'intérêt général.

La quatrième chose que je voulais dire pour terminer, c'est que plus il y a d'informations plus il y a d'incohérences et de rumeurs. Donc l'homme est

fou : il pense qu'un système d'information est plus rationnel et donc plus efficace, il oublie volontairement que, par définition, il y a énormément d'erreurs volontaires ou involontaires et d'incohérences dans les systèmes d'information. Et surtout que ce qui intéresse l'homme, c'est la rumeur, jamais l'information. Plus l'information est publique, plus il y a du secret. Plus nous serons dans une société de l'information, plus nous serons aussi dans une société de rumeur.

C'est important de rappeler, qu'en définitive, **plus il y a d'information, plus il y a de désordre**, parce qu'on pense exactement l'inverse. Les cybernéticiens nous avaient pourtant mis en garde, en mathématiques et même en biologie il y a une soixantaine d'années. Mais hélas, la perspective scientifique a été balayée par les performances techniques, justement parce que vous et moi nous sommes consommateurs, admirateurs et amoureux de ces informations, au sens où je l'ai dit tout à l'heure, parce qu'elle est le symbole de l'émancipation de l'homme depuis le XVIIe siècle.

Que faire pour éviter que ces deux conceptions antinomiques de l'information se rapprochent ? C'est la grandeur de la CNIL et de toutes les autorités de régulation de rappeler qu'il faut toujours que le législateur, ou le politique au sens large, ait le courage de dire que la problématique politique est toujours plus forte que la problématique économique ou technique. Nous n'y arrivons pas pour l'instant, mais il faut être optimiste.

Quand on a commencé à se battre en France pour l'exception culturelle en 1980 – après le terme est devenu plus « diversité culturelle » –, on a essayé de convaincre progressivement les pays européens et le reste du monde que la diversité culturelle était un enjeu politique pour la mondialisation. La vision française était considérée comme arrogante, stupide et égoïste. Nous venons de faire voter, pas nous, mais le monde entier, l'Unesco, à l'exception, vous le savez, d'Israël et les États-Unis, à la Conférence générale, le 20 octobre à Paris, ce principe fondamental, qui est une convention qui reprend la déclaration sur la diversité culturelle qui avait été votée en 2002, qui pose le principe du respect de la diversité culturelle dans la mondialisation. Bien sûr, ce n'est pas parce que l'Unesco vote une convention que ce sera respecté, mais cela veut dire que la conscience mondiale est en train de progresser le fait que la diversité culturelle est un enjeu de pays de guerre. Ce qu'on a réussi à faire en 20 ans sur les questions liées à la diversité culturelle, je ne vois pas pourquoi on arriverait pas à le faire sur la problématique des systèmes d'information ?

Donc, rappeler **qu'une problématique politique est toujours plus importante qu'une problématique technique ou économique**. Et même si les consommateurs ou les usagers trouvent qu'il ne faut pas réglementer, il faut rappeler cette chose toute simple : il n'y a pas de liberté d'information et de système d'information sans loi. La loi est toujours là pour protéger le faible et faire prévaloir l'intérêt général. Et ce sera aussi vrai pour les systèmes d'information que ce l'est aujourd'hui sur la presse écrite, sur la radio, sur les télécommunications, sur les satellites…

Pour faire naître plus facilement des problématiques critiques, il faut absolument préserver le pluralisme et faire du comparatisme. C'est-à-dire s'apercevoir que les cultures n'abordent pas de la même manière les rapports entre information, culture, émancipation, économie ou système symbolique, autrement dit faire du comparatisme, au sein de l'Europe, et donc *a fortiori* au niveau du monde. Donc favoriser le pluralisme culturel qui est un moyen de lutter contre la standardisation. On croit qu'en rationalisant et en standardisant, on est plus efficace ; en réalité, on reporte à plus tard les problèmes que la standardisation a éliminés. Le pluralisme ou le comparatisme, c'est apparemment du temps perdu ; c'est en fait une richesse pour demain. De même faut-il se battre pour le pluralisme linguistique. Tant que nous continuons sur les systèmes d'information et Internet, à baragouiner cet anglicisme dominant sans aucun respect des autres langues, nous ne faisons que succomber aux idéologies dominantes. Il faut parler des questions d'Internet dans sa langue naturelle. Il n'y a pas qu'une manière de parler l'Internet et par conséquent la défense du français, mais c'est vrai de la lusophonie, de l'hispanophonie, c'est vrai de l'arabophonie, c'est vrai de la russophonie, est absolument fondamentale. Admettre qu'il faut de la traduction. La traduction est la condition de la liberté. Ne pas traduire et parler une seule langue, ce n'est pas du tout la condition de la liberté, c'est simplement une fausse homogénéisation culturelle, qui de toute façon sera critiquée bien sûr. Je rappelle quand même qu'il s'est passé en 1980 à l'Unesco, un enjeu politique majeur, dont on n'a pas pris conscience et qui va revenir, c'était le débat sur le nouvel ordre mondial de l'information et des communications, le nomic… Les pays du Sud à l'époque dits socialistes avaient contesté les Occidentaux pour dire « votre société de l'information, c'est une conception impérialiste ». Je vous rappelle que dans ce nomic de 1980, nous les Occidentaux, nous avons gagné, parce que nous avons rapidement fait comprendre aux Soviétiques et aux pays du Sud, que, peut-être, on pouvait critiquer notre conception de l'information, mais qu'il fallait d'abord qu'ils arrivent eux-mêmes à une conception démocratique. Nous sommes vingt ans après, dans un contexte politique qui n'a plus rien à voir, le Nord/ Sud existe évidemment toujours et nous avons beaucoup moins de possibilités de défendre une conception pluraliste de l'information, face aux assauts, plus ou moins de bonne intention, qui sont faits contre une conception occidentale de l'information , perçue de plus en plus dans le monde comme un impérialisme. C'est en cela que le détournement chinois est très intéressant, mais je pourrais parler de l'Inde aussi et d'autres pays : il peut tout à fait y avoir la présence des mêmes systèmes d'information avec derrière des antagonismes radicaux sur les philosophies de l'information et de la communication.

Par ailleurs, **il faut absolument rappeler, et de plus en plus, la différence de ce qu'est une information par rapport à une communication**. Les systèmes d'information permettent la vitesse, la communication c'est lent, parce que ce sont automatiquement des hommes, des cultures, des idéologies et ce ne sont pas des systèmes techniques. Et donc plus les systèmes d'information sont rapides, performants et rationnels, plus il faut rappeler qu'au bout des systèmes d'information, ce sont des hommes, des sociétés, des cultures, et ça, ça évolue lentement, extrêmement lentement, mais après tout ce sont les hommes et les sociétés qui font la paix et la guerre et pas les systèmes d'information. Du coup, après la différence de nature ente la rationalité et l'efficacité d'une information d'une part, de

la complexité et la lenteur de la communication d'autre part, c'et aussi se donner les moyens de se garantir plus tard une possibilité de débat contradictoire sur la nature de l'information.

Enfin, dans les rapports entre information et communication, rappeler qu'évidemment la communication a un intérêt gigantesque par rapport à l'information, mais aussi **rappeler la complexité de ce qu'on appelle l'expérience**. Finalement agir, travailler, produire, vendre, ce sont des catégories d'expérience, qui sont naturellement beaucoup plus compliquées à mettre en ligne que les catégories de l'information. Autrement dit, si les systèmes interagissent ou font des interconnexions, seuls les hommes et les sociétés sont capables de faire de l'intersubjectivité. Quand on passe du côté de l'intersubjectivité, on passe nécessairement du côté de la communication avec tout ce que les sociétés portent derrière de valeurs, d'idéologies.

Ce qui fascine tous les historiens de la politique, et tous ceux qui ont fait de l'anthropologie politique, c'est qu**'il n'y a aucun rapport entre la rationalité d'un système d'information et une adhésion politique**. Il faut le répéter parce qu'il y a quand même dans notre idéologie politique, un paradigme, lui aussi assez simple, faux mais simple, qui consiste à dire qu'une bonne décision est une décision qui repose sur de bonnes informations. C'est ce qu'on apprend à l'école, ce qu'on apprend dans le management, ce qu'on apprend à l'ENA, bref ce qu'on apprend partout. Et ce que constate chaque individu dès qu'il a du pouvoir, c'est que naturellement il faut de l'information pour prendre une décision, mais, prendre une décision, ça nécessite d'autres valeurs que d'avoir de bonnes informations. Mais comme c'est plus simple de théoriser, de produire et de vendre des systèmes d'information que de réfléchir sur les conditions de l'action et de la décision, on est quand même dans ce continuum simple à savoir que si, finalement il y avait plus de systèmes d'informations, plus d'interconnectés, plus d'interactif, on aurait de meilleures décisions ! Il se trouve que les hommes sont à la fois capables de faire de superbes systèmes d'information rationnels *et* d'être complètement fous dans leurs décisions. L'histoire de l'humanité le prouve tous les matins. Donc l'important c'est de réfléchir sur la difficulté et la folie de la décision politique On le sait hélas par l'histoire ou par toute l'utilisation des fichiers : dès qu'un système politique se met à sortir des gonds, il a tous les moyens pervers d'utiliser les systèmes d'information à sa propre folie. Donc il est une question démocratique fondamentale qui est, évidemment, de limiter le plus possible l'existence de ces bases et de ces banques de données permanentes et surtout de **retirer cette idée apparemment rationnelle et simple qu'après tout accumuler des informations sur un individu n'est pas antidémocratique**. C'est contradictoire avec une problématique politique et démocratique, parce qu'on sait toujours par l'histoire, que quelle que soit la nature des bases de données, le pouvoir politique quand il devient totalitaire, sait récupérer les bases de données et s'en servir à sa faveur. On retrouve là, qu'il s'agisse d'Internet ou de bases de données en carton avec des fiches comme on les a vues pendant l'Occupation, comme on l'a vu dans le système soviétique, comme on le voit aujourd'hui en Chine. On sait très bien qu'il y a un lien direct tout de même, entre la capacité d'un pouvoir politique à utiliser les systèmes d'information et à les utiliser à sa convenance, c'est-à-dire la plupart du temps, hors des valeurs démocratiques.