

Faculté de droit

Année :

N° attribué par la bibliothèque

2003

MEMOIRE DE DEA INFORMATIQUE ET DROIT

Sous la direction

De Monsieur le Professeur Jean Frayssinet

**Les Fournisseurs d'accès à Internet, les fournisseurs
d'hébergement et les données à caractère personnel**

Présenté par :

Cedric HERBIN

Formation doctorale : Informatique et Droit
Equipe de Recherche Informatique et Droit (E.A. 2997)
Section CNU : Droit privé et sciences criminelles. 71 Sciences de l'information et de la communication.

E.R.I.D.

Remerciements

*A Monsieur le professeur Jean Frayssinet pour son
attention et sa célérité dans ses réponses et conseils*

*A Monsieur Michel Bibent pour m'avoir permis
de passer une année enrichissante*

Résumé

Les fournisseurs d'accès à Internet et les fournisseurs d'hébergement sont à un point stratégique afin de lutter contre les dérives d'Internet car ils détiennent de nombreuses données à caractère personnel sur leurs clients ou sur des visiteurs. Cette position cruciale justifie qu'au-delà des règles de droit commun et protectrices des données à caractère personnel, des dispositions spécifiques aménagent le régime des données à caractère personnel en leur possession en les obligeant à la fois à conserver ces données mais aussi à les révéler sur la demande des autorités. Les fournisseurs d'accès à Internet et les fournisseurs d'hébergement se trouvent donc dans un domaine où les données à caractère personnel sont moins protégées que pour le droit commun.

Index

Fournisseur d'accès à Internet, fournisseur d'hébergement, données à caractère personnel,
protection de la vie privée

Internet service provider, hosting provider, personal data, protection of privacy

**Les fournisseurs d'accès à Internet et les fournisseurs
d'hébergement et les données à caractère personnel.**
Mémoire de D.E.A. Informatique et Droit
Sous la direction du professeur Jean Frayssinet

Plan général

Première Partie : L'application des lois générales aux fournisseurs d'accès et aux fournisseurs d'hébergement

Section 1 : des sources diverses et variées

Paragraphe 1 : La protection des données à caractère personnel

Paragraphe 2 : La protection des correspondances et de la vie privée

Section 2 : Un régime protecteur des données à caractère personnel

Paragraphe 1 : Le contenu de la protection des données à caractère personnel

Paragraphe 2 : La protection par le secret

Seconde Partie : Un régime spécial qui aménage les dispositions protectrices

Section 1 : Les obligations de conserver les données à caractère personnel

Paragraphe 1 : L'obligation du fournisseur d'hébergement

Paragraphe 2 : L'obligation du fournisseur d'accès à Internet

Section 2 : Les obligations de divulguer les données à caractère personnel

Paragraphe 1 : Les réquisitions judiciaires

Paragraphe 2 : Les textes à venir

Introduction

Les données à caractère personnel, la vie privée, voici des expressions qui hier encore n'étaient réservées qu'aux juristes et qui peu à peu apparaissent comme un sujet digne d'intérêt par le grand public qui prend lentement conscience de leur importance. L'actualité est en effet marquée par de nombreuses problématiques liées aux données à caractère personnel. Alors lorsque les Etats-Unis réclament, au nom de la lutte anti-terroriste, un accès aux données des fichiers des compagnies aériennes, les médias se saisissent du dossier et l'opinion publique semble découvrir le problème.

Pourtant le problème n'est pas récent et n'a pas attendu le développement récent des nouvelles technologies, puisque la loi française sur le sujet date de 1978. Mais le développement des nouvelles technologies de l'information et de la communication a propulsé ces problématiques sur le devant de la scène, par l'importance des données à caractère personnel qui transitent sur ces réseaux et par la facilité des traitements relatifs à ces données au moyen de l'informatique.

En effet la puissance de l'outil informatique permet de traiter des données à caractère personnel de façon automatisée très rapidement mais surtout permet de traiter des volumes de données qui n'auraient pas pu l'être manuellement. Mais au-delà du traitement même des données, les nouvelles technologies permettent la collecte de données de façon massive, notamment chez certains prestataires techniques.

Les intermédiaires techniques que sont les fournisseurs d'accès à Internet et les fournisseurs d'hébergement disposent, en raison leur fonction, d'un accès à de nombreuses données qui transitent sur leurs matériels, ces données sont particulièrement sensibles car elles concernent tous les comportements des internautes lors de leur navigation, et part là même sont particulièrement intéressantes si l'on envisage une utilisation commerciale de ces données.

On voit donc la problématique concernant les libertés des individus qui transparaît derrière l'étude du régime juridique relatif à la protection des données à caractère personnel dans le domaine des nouvelles technologies.

Un sujet tel que «fournisseurs d'accès à Internet, fournisseurs d'hébergement et données à caractère personnel » ne pose pas de problème particulier d'interprétation, les trois notions ne sont pas ambiguës ni polysèmes. La notion de données à caractère personnel fera l'objet d'un développement particulier dans notre premier chapitre en raison de l'importance de cette notion.

La loi de 1986 relative à la liberté de communication décrit successivement les deux types d'activités dans ses articles 43-7 et 43-8.

L'article 43-7 concerne les fournisseurs d'accès à Internet qu'elle décrit comme « *Les personnes physiques ou morales dont l'activité est d'offrir un accès à des services de communication en ligne* », il s'agit ici des prestataires de service qui proposent aux particulier de servir d'intermédiaire afin de les relier à un réseau à l'échelle mondial qu'est Internet. Leur activité est en pratique d'interconnecter l'ordinateur du particulier aux infrastructures techniques d'Internet.

L'article 43-8 est lui relatif aux fournisseurs d'hébergement : « *Les personnes physiques ou morales qui assurent, à titre gratuit ou onéreux, le stockage direct et permanent pour mise à disposition du public de signaux, d'écrits, d'images, de sons ou de messages de toute nature accessibles par ces services* ». Cette activité consiste en pratique à mettre à la disposition d'un client tout ou partie d'un ordinateur connecté en permanence à Internet afin que les internautes puissent accéder aux données stockées sur l'ordinateur du fournisseur d'hébergement.

Les termes de fournisseur d'accès à Internet et de fournisseur d'hébergement ne sont donc pas les termes officiels utilisés ni par la loi ni par les directives mais le terme qu'adopte le grand public pour désigner les prestataires des activités décrites dans les articles 43-7 et 43-8 de la loi de 1986. La directive de 2002 parle, elle, de « *fournisseur d'un réseau public de communications ou d'un service de communications électroniques accessible au public* » ce qui est plus large et regroupe les deux activités de fournisseur d'accès à Internet et de fournisseur d'hébergement.

Quelque soit les termes adoptés par les textes, on cerne bien que ces deux prestataires sont en réalité les prestataires incontournables de l'existence d'Internet, l'un car il permet l'accès au réseau et l'autre car il mets à disposition du public le contenu d'Internet. Toute navigation sur Internet implique le recours à ces deux prestataires, ce qui explique qu'ils voient circuler sur leurs réseaux des données sur un nombre très élevé d'internautes. Ils ont donc ceci en commun que prestataires indispensables du réseau, ils détiennent des informations précises sur tous les internautes utilisant leur infrastructure et ceci souvent sans le savoir.

Mais l'intérêt du sujet n'est pas dans la description des différents acteurs, il faut plutôt s'interroger sur la relation entre ces différentes notions. Le sujet s'interroge sur les relations entre d'une part deux types d'intermédiaires techniques que sont les fournisseurs d'accès à Internet et les fournisseurs d'hébergement et d'autre part les données à caractère personnel.

Les prestataires peuvent avoir deux comportements relatifs à ces données : leur collecte et leur utilisation, ces deux comportements amènent à des commentaires juridiques relatifs au régime applicable, ce sera donc le régime juridique concernant à la fois la collecte et l'utilisation des données à caractère personnel par les fournisseurs d'accès à Internet et les fournisseurs d'hébergement qui feront l'objet de notre étude.

Mais ce sera sans oublier que l'utilisation des données recouvre aussi leur transmission, leur communication à des tiers et que cet aspect peut parfois prendre une grande importance notamment que les destinataires de cette communication de données à caractère personnel sont des autorités étatiques.

En présence de telles données sensibles, la tentation de les utiliser à des fins commerciales par les prestataires techniques est importante. Il est donc nécessaire de voir comment de telles données dans un secteur touchant les technologies sont protégées par la législation en vigueur.

En effet, la loi informatique et libertés date de 1978, on peut alors s'interroger sur son adaptation aux développements récents des nouvelles technologies.

Alors que la législation à la fois nationale et internationale semble prendre en compte les nouvelles technologies dans leur relation avec les données à caractère personnel, on pourrait s'interroger sur l'intérêt de traiter de la question qui ne pourrait être que l'étude de la législation.

Cependant, le régime juridique des données à caractère personnel dans le cadre qui nous intéresse n'est pas soumis à un régime unique ou unifié, de multiples législations s'appliquent et il nous faut donc connaître les différentes règles applicables pour en connaître le régime. De plus, certains des textes applicables sont extrêmement récents et leur contenu est à la fois méconnu car encore peu appliqué et surtout flou car, comme la plupart des textes législatifs concernant des aspects techniques, le législateur utilise des notions qu'il ne définit pas. Enfin certains textes sont tout simplement incomplets, les décrets d'application se faisant attendre.

On voit donc que le sujet de ce mémoire loin d'être purement descriptif d'une législation, se doit d'éclaircir une situation juridique touffue afin de permettre de connaître le régime applicable.

Les législations sur la protection des données à caractère personnel sont nombreuses de part le monde, et beaucoup pourraient trouver à s'appliquer de part la nature transfrontière d'Internet, cependant l'objet de notre propos sera d'étudier le droit positif en France, que ce droit résulte de législations nationales, régionales (législation communautaire principalement) ou internationales. Nous écarterons donc systématiquement les législations qui ne sont pas du droit positif en France, tout en gardant à l'esprit qu'elles pourraient éventuellement trouver à s'appliquer en fonction de leurs champs d'applications territoriaux.

Il ne s'agit pas seulement d'établir les règles que devront respecter les fournisseurs d'accès à Internet et les fournisseurs d'hébergement, mais de constater au-delà de ces règles la volonté du législateur. En effet, les lois relatives aux données à caractère personnel ont ceci en commun qu'elles établissent un régime de protection de la personne fichée, c'est la raison d'être de ces lois. Les législateurs ont considéré que les données à caractère personnel et leurs traitements étaient des atteintes aux libertés et à la vie privée des individus et ont donc souhaité encadrer ces traitements.

Cependant les traitements de données à caractère personnel ont aussi des intérêts qui peuvent être très divers : il peut aussi bien s'agir des intérêts économiques des entreprises qui effectuent ces traitements que des intérêts étatiques de recherche d'auteurs d'infractions. Il faut donc trouver un juste équilibre entre la nécessité des traitements et la protection des individus qui font l'objet de ces traitements.

Le choix du régime juridique dans cette matière n'est donc pas sans importance, puisque le choix du régime aura pour conséquence d'augmenter ou de diminuer l'atteinte aux libertés et à la vie privée des individus.

Ce choix a lieu dans une période où le monde est frappé par une augmentation du terrorisme qui permet aux gouvernements de prendre, parfois à juste titre, des mesures portant atteinte aux libertés des citoyens pour des raisons de sécurité. Il convient donc de s'interroger sur la

pertinence des législations récentes sur les données à caractère personnel afin de constater leur incidence sur les libertés des individus.

Le sujet, à travers l'étude d'un régime juridique, fait transparaître aussi le caractère plus ou moins liberticide des législations relatives aux fournisseurs d'accès à Internet, aux fournisseurs d'hébergement et aux données à caractère personnel.

Comme le soulignait le professeur Jean Frayssinet lors d'un colloque¹, «il n'existe pas à proprement parler de système juridique de protection des données à caractère personnel, c'est à dire des droits et libertés des personnes, qui soit spécifique à l'Internet », en effet le droit semble indifférent à cet aspect technique particulier.

Ceci ne signifie pas que le droit ne se soit pas adapté pour suivre l'évolution des techniques mais il ne s'agit pas à proprement parler d'un système juridique particulier, il s'agit en réalité d'aménagements, d'adaptations du système existant.

Le cadre juridique est donc celui très large de la protection des données à caractère personnel qui fait l'objet d'un régime complet basé sur des textes à la fois nationaux et internationaux, il est complété par quelques textes sectoriels qui aménagent ce régime en ce qui concerne les fournisseurs d'accès à Internet et les fournisseurs d'hébergement.

Ceci signifie donc que lorsque l'on s'interroge sur les droits et obligations des fournisseurs d'accès à Internet et des fournisseurs d'hébergement, il est plus judicieux de consulter en premier lieu les textes de droit commun relatifs à la protection des données à caractère personnel et ensuite de vérifier que le régime prévu par les textes n'a pas été aménagé par des textes spéciaux.

Les fournisseurs d'accès à Internet et les fournisseurs d'hébergement étant soumis au régime juridique de droit commun relatif à la protection des données à caractère personnel, certains

¹Colloque « L'Internet et le droit » 25 et 26 septembre 2000, organisé sous l'égide de l'école doctorale de droit public et de droit fiscal de l'université Paris 1

traitements de ces données ne seront pas l'objet de notre propos, il s'agit de tous les traitements qui ne leurs sont pas spécifiques (les données concernant les salariés pour le paiement des salaires, les données destinées au marketing mais qui ne proviennent ni ne sont destinées à Internet, ...) cependant les règles de droit décrites dans notre premier chapitre relatif au régime de droit commun trouveront à s'appliquer à ces données, elles ne feront cependant pas l'objet de développements particuliers.

On se trouve donc en présence de l'application du droit commun qui s'applique aux données à caractère personnel à raison de leur nature propre (Première Partie). Mais l'évolution récente est marquée non pas par l'apparition d'un régime spécifique mais par l'émergence d'aménagements au régime de droit commun propres à l'activité des prestataires techniques que sont les fournisseurs d'accès à Internet et les fournisseurs d'hébergement (Seconde Partie).

Chapitre 1. L'application des lois générales aux fournisseurs d'accès et aux fournisseurs d'hébergement

Les données qui transitent par ces intermédiaires techniques que sont les fournisseurs d'accès et les fournisseurs d'hébergement ont un régime propre, indifférent à l'activité du prestataire qui assure leur transmission.

Les différents caractères des données justifient l'application de sources diverses et variées (Section 1) qui ont un objectif commun : un régime protecteur des données (Section 2).

Section 1. Des sources diverses et variées

Les données transmises par les prestataires techniques ont une nature complexe, elles peuvent entrer dans la notion de données à caractère personnel (paragraphe 1) mais aussi de correspondance privée (paragraphe 2)

§1. La protection des données à caractère personnel

On observe autant dans la législation nationale qu'internationale la présence de la notion de « traitements de données à caractère personnel » (A) qui fait l'objet de réglementations (B)

I. La notion de « traitements de données à caractère personnel »

A) La notion de données à caractère personnel

Les textes concernant la notion de données à caractère personnel sont relativement nombreux et hétérogènes, malgré tous apportent des définitions assez semblables de la notion de données à caractère personnel.

- *"Toute information concernant une personne physique identifiée ou identifiable"* (Convention du conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel)
- *"Toute information concernant une personne physique identifiée ou identifiable. Une personne physique n'est pas considérée comme "identifiable" si cette identification nécessite des délais, des coûts ou des activités déraisonnables."* (Recommandation n° R (83) 10 du Comité des ministres du Conseil de l'Europe sur la protection des données à caractères personnel utilisées à des fins de recherche scientifique et de statistiques, 1983, Annexe, art. 1-2
- *"Toute information concernant une personne physique identifiée ou identifiable; est réputée identifiable une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale."* (Directive CE du 24 octobre 1995)
- La loi de 1978 adopte une appellation différente des données à caractère personnel, qu'elle nomme «informations nominatives », et qu'elle définit ainsi : *« Sont réputées nominatives au sens de la présente loi les informations qui permettent, sous quelque forme que ce soit, directement ou non, l'identification des personnes physiques auxquelles elles s'appliquent, que le traitement soit effectué par une personne physique ou par une personne morale. »* (Article 4 de la loi informatique et libertés)

La définition adoptée par la directive est la définition la plus précise. On observe aussi que quel que soit le texte concerné, il existe une base commune qu'est l'information concernant une personne physique identifiée ou identifiable.

On peut alors s'interroger sur l'application de cette définition aux données dont disposent les fournisseurs d'accès à Internet et les fournisseurs d'hébergement afin de savoir celles qui entrent dans la catégorie des données à caractère personnel.

Certaines données sont clairement nominatives, c'est le cas notamment du *login*, qui est le pseudonyme sous lequel se connecte un client du fournisseur d'accès à Internet, cette donnée est communiquée systématiquement au fournisseur d'accès à Internet lors de l'établissement de la connexion. Le *login* est aussi utilisé par les fournisseurs d'hébergement pour identifier leurs clients lorsqu'ils envoient des données à leur fournisseur ou bien simplement lorsqu'ils s'identifient afin de consulter ou modifier les caractéristiques de leur hébergement. Le *login* apparaît comme anonymisé puisqu'il peut ne pas être le nom réel de la personne, cependant c'est clairement une donnée indirectement nominative puisque le fournisseur d'accès à Internet ou le fournisseur d'hébergement peut très facilement connaître le nom de son client auquel correspond le *login*.

La donnée la plus importante et la plus utilisée par les fournisseurs est l'adresse IP, celle-ci identifie de manière unique à un moment donné un ordinateur connecté à Internet ou à un réseau, cependant elle est susceptible de changer à chaque nouvelle connexion de l'ordinateur. Pour une personne située sur Internet qui capterait l'adresse IP d'un ordinateur, il est impossible de connaître l'identité de la personne correspondante, ce qui pourrait laisser à penser que l'adresse IP n'est pas une donnée à caractère personnel, de plus l'adresse IP correspond à un ordinateur et non pas à un utilisateur, plusieurs utilisateurs pouvant utiliser le même ordinateur.

Cependant les fournisseurs d'accès à Internet conservent pour un moment donné les relations entre une adresse IP et un *login*, ce qui permet donc à partir d'une date et d'une heure et d'une adresse IP de connaître l'identité du titulaire du compte utilisé pour la connexion. Il semble donc que l'adresse IP soit une donnée à caractère personnel indirectement nominative car rapprochée des fichiers du fournisseur d'accès à Internet elle permet d'identifier (au moins avec une probabilité très élevée) l'utilisateur de l'ordinateur.

En l'absence de décision jurisprudentielle en ce sens, nous pouvons nous référer aux avis des autorités compétentes en la matière qui considèrent l'IP comme une donnée personnelle. Tout d'abord la CNIL dans un avis non publié a énoncé que l'adresse IP était une donnée à caractère personnel, cependant dans une interview² un juriste de la CNIL rappelle que bien que la CNIL considère l'adresse IP comme une donnée à caractère personnel, cette opinion n'a pas de valeur normative et le juge saisi de la question peut suivre ou non cette opinion. Le groupe de travail sur

² Interview de Mathias Moulin, juriste à la CNIL, accordé à 01net le 24 février 2003

la protection des données de la Commission européenne considère lui aussi que les adresse IP sont des données à caractère personnel³ au sens de l'article 26 de la directive 95/46/CE. Elle se fonde sur le fait que le fournisseur de services peut toujours faire le lien entre l'adresse IP et l'identité de son client.

De plus l'évolution technologique va confirmer cette analyse, en effet un nouveau standard d'adresse IP dite IPv6 vise à attribuer de manière unique et définitive une adresse IP à un ordinateur, dans cette hypothèse il suffira aux entreprises de connaître une fois l'adresse IP correspondant à un individu pour pouvoir l'identifier par la suite par sa simple adresse IP.

B) La notion de traitement

Il est défini par l'article 2 de la directive et l'article 5 de la loi de 1978.

L'article 2.b de la directive de 1995 définit le traitement comme « toute opération faite, action opérée, sur des données à caractère personnel. »

Le mot traitement ne s'entend pas au sens informatique du terme, il a un sens spécifique à la directive, aux droits à la protection des données à caractère personnel. Certaines opérations ne seront pas des traitements pour des informaticiens mais le seront au sens de la directive.

Une seule opération suffit pour avoir un traitement. Il y a deux types de traitements : automatisé et manuel.

On voit bien que la notion de traitement est extrêmement large, elle recouvre toutes les opérations sur les données à caractère personnel. En pratique la mise en place d'un fichier de données à caractère personnel traduira l'existence d'un traitement.

Pour les fournisseurs d'accès à Internet et pour les fournisseurs d'hébergement, l'existence d'un traitement ne fait aucun doute puisque la simple collecte, l'enregistrement ou l'utilisation des données personnelles sont des traitements au sens de la loi et de la directive.

³ Groupe de Travail sur la protection des données de la commission européen dit groupe « article 29 », Avis 2/2002 relatif à l'utilisation d'identifiants uniques dans les terminaux de télécommunication : exemple de l'IPv6, adopté le 30 mai 2002.

Les fournisseurs d'accès à Internet et les fournisseurs d'hébergement sont donc clairement les responsables de traitements de données à caractère personnel justifiant l'application des législations relatives à ces données.

II. Les lois « informatiques et libertés »

Dès les années 1970 apparaissent les premiers débats relatifs à l'informatique notamment les débats sur le secteur public, en vue de la protection des données à caractère personnel.

Le land de Hesse (Allemagne) en 1970 est le premier à adopter ce genre de texte ainsi qu'une loi suédoise de 1973, les Etats-Unis suivent avec en 1974 le *privacy act*.

En France, le texte de base est la loi du 6 janvier 1978. Cette loi est née de l'inquiétude générale relative au fichage informatique.

Un certain nombre de problèmes vont servir de déclencheurs : le projet d'informatisation du secteur de la santé, le projet GAMIN et le projet SAFARI.

Bien que tous les pays ne disposent pas de réglementation relative aux données à caractère personnel, la France dispose depuis longtemps de législations les concernant. Mais d'autres sources législatives concernent ces données.

A) La législation nationale

La Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés dite «loi Informatique et Libertés » est la loi qui fixe le droit commun du droit des données à caractère personnel. C'est une loi très complète et qui a inspiré d'autres législations notamment communautaires.

B) La législation régionale et internationale

Le droit communautaire n'est *a priori* pas compétent, car la question des données à caractère personnel n'entre pas dans son champ de compétences. Ce problème a été contourné par le biais du marché et du principe de libre circulation des biens et services et des personnes sur le marché unique car un certain nombre de pays s'étaient dotés de lois sur la protection des données à caractère personnel alors que d'autres n'avaient rien ou des lois insuffisantes, or les données à caractère personnel circulent sur le territoire de l'union européenne, ces données se vendent, s'achètent, ce sont des biens. Alors qu'à l'origine, il s'agit d'une approche relative aux droits de la personnalité (personne ne dispose de ces informations, pas même le fiché) l'approche communautaire a pratiqué une patrimonialisation qui impose d'appréhender les données comme un bien, une marchandise. Or comme il existait des législations différentes, il pouvait exister une distorsion de concurrence justifiant la compétence communautaire.

La directive 95/46 du 24 octobre 1995 « relative à la protection des personnes physiques à l'égard du traitement automatisé des données à caractère personnelles et à la libre circulation de ces données » établit une compétence pour un aspect de marché mais aussi pour l'aspect droit des personnes, c'est à dire sous un aspect de droits et libertés (apport des traités de Maastricht et Amsterdam)

La directive ne concerne pas ce qui est attaché à la souveraineté de l'Etat (art. 3-2).

Le principe énoncé par la directive est une libre circulation des données à caractère personnel sur le territoire à condition de respecter les droits nationaux qui doivent au minimum transposer les règles de la directive.

La transposition devait survenir dans les trois ans. Tous les états ont transposé à l'exception de la France et en partie de l'Allemagne. Les raisons sont diverses : la France est en générale peu rapide dans les transpositions, il s'agit d'une transposition compliquée car elle concerne beaucoup de ministères, il s'agit d'un texte sensible pour l'opinion publique et donc sensible d'un point de vue politique puisqu'il y avait toujours des échéances électorales.

A présent la France tarde dans la transposition car elle avait certaines lois à faire passer assez contraires à l'esprit de la directive notamment la loi sur la Sécurité Quotidienne

La directive 2002/58 du 12 Juillet 2002 « concernant le traitement des données à caractère personnelles et la protection de la vie privé dans le secteur des communications électroniques » dite « vie privée et communication électroniques » vient remplacer la directive 97/66 du 15 décembre 1997 qui devait être transposée en octobre 1998. Il s'agit d'une directive sectorielle, spécialisée concernant le secteur des communications électroniques. C'est aussi une directive fille de la directive 95/46 d'octobre 1995.

On trouve aussi des règles relatives aux données à caractère personnel dans des directives dont ce n'est pas l'objet principal comme la directive « Commerce Electronique ».

La charte des droits fondamentaux a été adoptée pendant la convention de Nice le 7 décembre 2000 et devrait être intégrée comme préambule à une éventuelle constitution. Les articles 7 et 8 de la charte concerne les données à caractère personnel. Certains pays ont déjà consacré au niveau constitutionnel la protection des données à caractère personnel (Espagne, Portugal, ...)

Convention 108 du 28 janvier 1981 relative à la protection des personnes à l'égard du traitement automatisé des données à caractère personnelles, conçue dans le cadre du conseil de l'Europe : c'est une convention signée et ratifiée par la France entrée en vigueur le 1 octobre 1985, elle est ouverte à l'adhésion de pays non-membres du conseil de l'Europe Cette convention est un texte international qui engage la France, l'article premier affirme les libertés à protéger pour toutes les personnes physiques : respect des droits et libertés fondamentaux et notamment le droit à la vie privée par rapport au traitement des données à caractère personnel la concernant.

Cette convention a été une source d'inspiration de la directive de 1995. L'intégration de cette convention en droit français a été reconnue à plusieurs reprises par le Conseil d'état⁴, on peut donc invoquer directement la convention 108.

Il existe un protocole additionnel sur les autorités de contrôle et les flux transfrontières de données du 8 novembre 2001. Il existe un amendement à la convention afin de permettre l'adhésion à la convention 108 des communautés européennes.

⁴ arrêt Licra, CE, 18/11/1992 et Arrêt CGT, 28/07/1995

A coté de la convention 108, le conseil de l'Europe a élaboré des recommandations sans valeur normative sur la protection des données à caractère personnel dans une approche sectorielle. Il existe notamment des *GuideLines* de l'OCDE de 1980, ainsi qu'une recommandation du 9 décembre 1999 relative aux lignes directrices pour le consommateur dans le contexte du commerce électronique.

L'ONU a adopté une résolution : lignes directrices relatives à la protection des données à caractère personnel qui n'a pas non plus de valeur normative.

L'accord du 15/04/1994 de l'Organisation Mondiale du Commerce prévoit que l'on peut limiter les règles favorisant le commerce si les dispositions nationales tendent à la protection de la vie privée pour le traitement et la circulation des données à caractère personnel.

Dans le monde, une cinquantaine de pays ont une législation nationale. Les États-Unis n'ont pas de loi fédérale comparable, mais une multitude de textes au niveau des états fédérés et des lois fédérales sectorielles (banque, assurance)

L'arsenal juridique est varié, le droit de la protection des données à caractère personnel n'en est qu'un élément, on peut aussi avoir recours au droit à la vie privée, au droit à l'image, au droit à la voix, au droit au nom, qui sont des droits de la personnalité (droits subjectifs). Il est nécessaire de faire des connexions entre la protection des données à caractère personnel et les droits subjectifs. La protection des données à caractère personnel a comme objet notamment la protection de la vie privée, il existe aussi des protections de droit pénal tels que la protection du secret professionnel ou la sanction de certaines atteintes au droit à la vie privée. Il existe aussi des règles sectorielles, par exemple un décret de janvier 2002 relatif aux données présentes dans les annuaires.

§2. La protection des correspondances et de la vie privée

I. Le secret des télécommunications et des correspondances

Les correspondances émises par la voie des télécommunications disposent depuis la loi du 10 juillet 1991⁵ d'un régime propre, auparavant elles étaient protégées par des lois non spécifiques telles que les dispositions relatives à la vie privée notamment.

La loi du 10 juillet 1991 introduit donc un principe général de secret des correspondances émises par la voie des télécommunications.

Ce principe s'applique à l'ensemble des correspondances transmises par la voie des télécommunications ce qui englobe les réseaux informatiques et par-là même le réseau Internet.⁶

Le secret des correspondances est aussi consacré par des conventions internationales :

- La convention internationale des télécommunications dispose dans son article 22 : « *Les membres s'engagent à prendre toutes les mesures possibles, compatibles avec le système des télécommunications employé en vue d'assurer le secret de la correspondance.* »
- La convention européenne des droits de l'homme protège aussi dans son article 8 le droit de toute personne au respect de sa vie privée et familiale, de son domicile et de sa correspondance. Ce fondement a été déjà utilisé par la cour européenne des droits de l'homme afin de protéger le secret des correspondances⁷

La législation sur le secret des correspondances concerne donc les fournisseurs d'accès à Internet ainsi que les fournisseurs d'hébergement car ces deux prestataires sont susceptibles de voir circuler sur leurs réseaux mis à dispositions de leurs clients des communications qui sont des correspondances au sens de la législation.

II. La vie privée

⁵Loi n°91-646 du 10 juillet 1991.

⁶Rapp. L., Le courrier électronique, PUF, 1998, Que sais-je?, n°3409, p.89.

⁷Arrêt Klas, 6 septembre 1978; Arrêt Malon, 2 août 1984; Arrêt Huvig et Kruslin, 24 avril 1990.

En droit français, la déclaration des droits de l'homme garantie certaines libertés, et la vie privée se trouve dans le Code Civil. On peut se demander quelle place a la vie privée dans la hiérarchie des normes. D'abord on a rapproché la vie privée de la liberté individuelle, contenue dans la constitution. Le conseil constitutionnel dans une décision DC 23/07/1999, Couverture Maladie Universelle, a estimé que la vie privée se rattache à l'article 2 de la déclaration des droits de l'homme de 1789 c'est à dire la notion de liberté personnelle. Le juge donne un statut constitutionnel à la vie privée et cela permet de reconnaître la compétence du juge administratif (alors que ce n'est pas le cas en matière de liberté individuelle)

Le conseil constitutionnel a estimé que le droit à la protection des données à caractère personnel se rattache à la liberté individuelle dans une décision du 20/01/1993 par la même opération que pour la vie privée. C'est une constitutionalisation indirecte *a priori*.

La loi reformant la loi informatique et libertés qui va être votée dans quelques mois sera soumise au conseil constitutionnel (alors que la loi de 1978 n'y avait pas été soumise), il s'agit d'un grand texte politique.

On ne peut pas diminuer le niveau de protection des droits et libertés, de même on protège le statut de la CNIL.

La Convention Européenne de Sauvegarde des Droits de l'Homme ne contient pas de dispositions particulières mais son article 8 traite de la vie privée : la cour européenne de sauvegarde des droits de l'homme a connu du contentieux touchant à la protection des données à caractère personnel par le biais du droit à la vie privée : arrêt M.S. Contre Suède sur la présence du nom des parties dans les décisions de justice.

Dans les arrêts CEDH, 16/02/2000 Amann contre Suisse et CEDH, 04/05/2000, Roturm contre Roumanie, la CEDH a estimé que des données à caractère personnel relatives aux activités politiques publiques et passées du requérant, détenues et traitées par les services de sécurité intérieure roumains relevaient de la vie privée.

En ce qui concerne le **droit communautaire**, l'article 6 alinéa premier du traité UE pose "l'union est fondée [...] sur le respect des droits de l'homme et des libertés fondamentales". La directive de 1995 fait référence explicitement à la Convention européenne de sauvegarde des droits de

l'homme, bien que l'union européenne estime ne pas pouvoir en être membre. L'article 6 alinéa 2 du traité UE dispose que l'union européenne respecte les droits de l'homme et les libertés fondamentales tels qu'ils sont garantis par la Convention européenne de sauvegarde des droits de l'homme, il s'agit ici d'une façon d'intégrer la Convention européenne de sauvegarde des droits de l'homme, cependant il faut être prudent car des interprétations divergents existent entre la Cour de Justice des Communautés européennes et la Cour européenne de sauvegarde des droits de l'homme.

On voit donc que les données à caractère personnel transmises sur les réseaux du fournisseur d'accès à Internet comme ceux du fournisseur d'hébergement peuvent aussi être protégées par la législation relative à la vie privée.

Les données que peuvent intercepter les fournisseurs d'accès à Internet et les fournisseurs d'hébergement peuvent donc être appréhendées de manières diverses par le droit permettant ainsi une superposition des régimes applicables à ces données. Cependant on peut constater une certaine homogénéité dans les objectifs de ces régimes : ils sont tous extrêmement protecteurs des données concernées.

Section 2. Un régime protecteur des données à caractère personnel

Les données ainsi définies sont donc soumises à des régimes multiples qui ont pour point commun un aspect protecteur des données à caractère personnel, et ce à la fois au moyen de la loi « informatique et libertés » (paragraphe 1) et par le secret (paragraphe 2)

§1. Le contenu de la protection des données à caractère personnel

La protection des données à caractère personnel passe par deux grands mécanismes : des obligations à la charge du fournisseur d'accès à Internet ou du fournisseur d'hébergement responsable du traitement des données (I) , et des droits au bénéfice de l'internaute fiché (II)

I. – Les obligations des fournisseurs d'accès à Internet et des fournisseurs d'hébergement relatives au traitement des données à caractère personnel

A) Le régime d'autorisation / déclaration

a) Le régime d'autorisation

Ce régime concerne les traitements opérés pour le compte d'une personne publique (Etat, établissement public, collectivité territoriale, personne morale de droit privé gérant un service public).

Ce régime prévu par l'article 15 de la loi « informatique et liberté » impose que la décision de mettre en place un traitement de données à caractère personnel soit prise par un acte réglementaire après avis motivé de la Commission Nationale Informatique et Libertés.

Si la Commission Nationale Informatique et Libertés donne un avis favorable, l'acte réglementaire peut être pris et le traitement mis en place.

Si la Commission Nationale Informatique et Libertés donne un avis défavorable, il sera possible d'aller à l'encontre de cet avis au moyen d'un décret pris sur avis conforme du Conseil d'état.

Cette procédure semble concerner *a priori* peu les fournisseurs d'accès à Internet et les fournisseurs d'hébergement, cependant elle n'est pas à exclure car le secteur public peut très bien pratiquer ce genre d'opérations. Une collectivité territoriale peut, par exemple, proposer un hébergement pour sa promotion.

b) Le régime de déclaration

Lorsqu'un traitement est effectué par une personne privée, le régime n'est plus un régime de contrôle *a priori* mais une simple déclaration préalable prévu par l'article 16 de la loi « informatique et liberté »

Il s'agit alors simplement pour le responsable du traitement de déclarer à la commission nationale informatique et liberté la mise en place du traitement au moyen d'un formulaire qui vise à connaître les différentes caractéristiques du traitement.

Dans cette déclaration, le responsable du traitement de données à caractère personnel s'engage à ce que son traitement respecte les exigences légales.

La Commission Nationale Informatique et Libertés délivre alors, sans délai, un récépissé au responsable du traitement qui peut alors mettre en œuvre le traitement.

Ce régime peut paraître inutile cependant il permet en réalité à la Commission Nationale Informatique et Libertés comme aux utilisateurs de connaître l'existence des traitements et leur contenu. Ceci est aussi un moyen d'information pour la Commission Nationale Informatique et Libertés.

La plupart des fournisseurs d'accès à Internet ainsi que la plupart des fournisseurs d'hébergement étant des personnes de droit privé, c'est le régime de la déclaration préalable qui sera la procédure la plus fréquemment utilisée dans la pratique.

B) Les obligations du maître des fichiers

Le régime mis en place par la loi informatique et libertés, fixe un certain nombre d'obligations à l'encontre du responsable du traitement, afin de protéger la personne fichée.

a) Le principe de finalité

Lors de la déclaration, le responsable du traitement, ici le fournisseur d'accès à Internet ou bien le fournisseur d'hébergement devra déclarer la finalité de son traitement, or le choix d'une finalité n'est pas purement accessoire, il va lier le responsable du traitement, qui ne pourra pas utiliser les données à caractère personnel au-delà de la finalité déclarée.

En effet, pour le maître du fichier, l'utilisation des données hors du cadre de la finalité déclarée constitue une infraction pénale.

Ceci permet à la personne fichée de s'assurer de l'utilisation qui sera faite de ses données, en effet lorsqu'un traitement sera fait à son sujet il sera informé et pourra donc connaître la finalité du traitement, l'interdiction d'utiliser les données en dehors de leur finalité déclarée lui permettra de savoir que ses données ne sortiront pas de la finalité dont il a pris connaissance.

Il est donc très important pour les fournisseurs d'accès et d'hébergement de bien déterminer les finalités lors de la déclaration à la Commission Nationale Informatique et Libertés, car ils ne pourront pas s'en éloigner.

Le seul moyen de s'éloigner de la finalité déclarée est de faire une nouvelle déclaration mais la déclaration n'a pas d'effet rétroactif.

b) L'obligation de sécurité

L'article 29 de la loi Informatique et Libertés dispose que « Toute personne ordonnant ou effectuant un traitement d'informations nominatives s'engage de ce fait, vis-à-vis des personnes concernées, à prendre toutes précautions utiles afin de préserver la sécurité des informations et notamment d'empêcher qu'elles ne soient déformées, endommagées ou communiquées à des tiers non autorisés. »

On est ici, dans le cadre des obligations des fournisseurs d'accès à Internet et des fournisseurs d'hébergement, en présence d'une obligation majeure. En effet, nous l'avons vu les fournisseurs d'accès à Internet et les fournisseurs d'hébergement disposent d'informations qui permettent l'identification indirecte de leurs clients, or si ces informations sont modifiées, perdues ou communiquées à des tiers, les conséquences peuvent être importantes.

Dans le cadre d'une procédure judiciaire, si les informations sont modifiées une personne pourra se voir poursuivie et opposer des preuves qui seront techniquement crédibles mais erronées, alors la charge de la preuve incombera à l'internaute poursuivi qui aura bien du mal à prouver sa bonne foi. De même si les informations sont perdues, alors il sera impossible de rechercher l'auteur d'une infraction.

La communication à des tiers de données détenues par les fournisseurs d'accès à Internet ou les fournisseurs d'hébergement est, elle aussi, problématique car les fichiers d'un fournisseur d'accès à Internet par exemple permet de connaître l'équivalence entre une adresse IP et une personne. Ces fichiers peuvent aussi contenir les coordonnées bancaires, ou bien tout simplement être des fichiers de prospects commerciaux très intéressants.

Le problème est d'autant plus complexe à gérer pour les fournisseurs d'accès à Internet et les fournisseurs d'hébergement que leur activité leur impose d'être connectés de manière constante sur Internet et ils font donc une cible de choix pour les piratages.

Il s'agit, à suivre les termes de la loi, d'une obligation de moyens. Le fournisseur d'accès à Internet et le fournisseur d'hébergement étant des professionnels de l'informatique, ils vont devoir mettre en œuvre des moyens très importants pour assurer leur sécurité.

Cependant, il semble que ces prestataires soient assez efficaces, puisque les piratages de données à caractère personnel chez ceux-ci semblent assez rares ou bien occultés systématiquement.

c) La durée de conservation

La loi 78-17 prévoit dans son article 28 que les informations ne peuvent pas être conservées sous une forme nominative au-delà de la durée prévue dans la déclaration ou la demande d'avis. Cependant la Commission Nationale Informatique et Libertés peut autoriser leur conservation.

L'article 226-20 du Code Pénal prévoit une sanction pénale à une violation de ces obligations, en condamnant à 3 ans de prison et 45 000 euros d'amende, celui qui conserve les informations nominatives au-delà de la durée prévue.

Les fournisseurs d'accès devront penser lors de la déclaration à fixer une durée raisonnable

Au-delà de cette durée fixée par le responsable du traitement lui-même, certains textes imposent des durées maximales de conservation dans certains domaines, c'est ce que nous verrons plus tard dans le cadre du régime aménagé pour les prestataires intermédiaires.

Mais la limite de conservation dans le temps n'est pas seulement la durée déclarée lors de la procédure de déclaration à la CNIL car l'article 28 de la loi IL dispose « Au-delà de la durée nécessaire à la réalisation des finalités pour lesquelles elles ont été collectées ou traitées, les informations ne peuvent être conservées sous une forme nominative qu'en vue de leur traitement à des fins historiques, statistiques ou scientifiques. » par conséquent, la fixation de la finalité est très importante, car l'interprétation de celle-ci permettra de limiter la durée de conservation.

d) L'obligation d'information

Cette obligation a pour but d'établir une certaine transparence, elle est prévue par l'article 27 de la loi de 1978 et les articles 10 et 11 de la directive de 1995.

Les fournisseurs d'accès à Internet et les fournisseurs d'hébergement responsables du traitement doivent donner des informations aux personnes concernées. Ces informations doivent permettre à la personne concernée de connaître l'existence du traitement et donc de mettre en œuvre tous ses droits relatifs au traitement des données à caractère personnel.

Dans le cas de la relation directe entre le fournisseur d'accès à Internet ou le fournisseur d'hébergement et son client (article 10 de la directive), il s'agit en premier lieu d'une obligation d'information pour la collecte auprès de la personne concernée, sauf si la personne a déjà été informée. L'information concerne l'identité du responsable du traitement, les finalités du traitement et des informations supplémentaires telles que destinataires ou catégories de destinataires, le caractère obligatoire ou facultatif des réponses, ainsi qu'une information sur l'existence du droit d'accès et de rectification.

La loi de 1978 précise que lorsque ces informations sont recueillies par voie de questionnaire : ceux-ci doivent porter mention de ces prescriptions. Le texte d'application prévoit que tout questionnaire sans ces mentions est passible d'une contravention de 5ème classe par questionnaire.

Si le fournisseur d'accès à Internet ou le fournisseur d'hébergement cède ces données, il est nécessaire que la personne dont les données cédées soit informée. Cette obligation n'est pas prévue par la loi de 1978 mais seulement par la directive qui ne précise pas qui doit informer l'internaute dont les données sont cédées. Il faudra donc prévoir, dans le contrat de cession, qui devra informer, ce qui pourra augmenter le coût de la cession.

Cette obligation crée un élément de traçabilité des données.

Cette règle ne s'applique pas lorsqu'il s'agit de finalités statistiques, scientifiques ou bien quand le coût est disproportionné ou lorsque l'effort est disproportionné. Cette exception est très intéressante lorsqu'un fournisseur d'hébergement laisse à la charge d'un prestataire le soin de faire des statistiques sur les accès au site, car s'agissant d'un traitement statistique on pourra donc faire jouer l'exception.

II. Les droits de l'internaute fiché

L'internaute dont les données sont collectées et utilisées par les fournisseurs d'accès à Internet ou les fournisseurs d'hébergement doit avoir la capacité contrôler ce qui est fait des informations la concernant et leur qualité, cette personne doit avoir une attitude active dans l'exercice de ses droits.

Ces droits ne fonctionnent pas de manière satisfaisante dans la pratique, la France fait partie des pays les plus passifs dans la pratique. De plus bien des personnes ignorent que des données sont collectées et utilisées par leur fournisseur d'accès à Internet ou les fournisseurs d'hébergement, faute d'information de ceux-ci.

L'objectif premier est donc de permettre ce contrôle par une mise en place de mécanismes, d'un enchaînement de droits.

A – Le droit de s'informer

Ce droit est prévu par l'article 34 de la loi de 1978 et par l'article 12 de la directive de 1995.

Il s'agit en pratique de poser la question « traitez vous des données personnelles me concernant ? »

C'est un droit à la curiosité qui n'est subordonné à aucune condition, tout internaute peut donc interroger un fournisseur d'accès à Internet ou un fournisseur d'hébergement sur le sujet.

Si le responsable refuse de répondre à la demande, il s'expose à une contravention de 5ème catégorie.

Ce n'est pas un droit collectif mais personnel, sauf pour un mineur par exemple.

L'internaute peut formuler sa demande par tout moyen et la réponse doit être gratuite pour celui-ci.

B – Le droit d'accès à l'information

Ce droit est prévu par l'article 35 de la loi de 1978 et l'article 12 de la directive qui prévoient que toute personne a le droit d'accéder à toutes les données personnelles le concernant, et faisant l'objet d'un traitement. C'est un des droits qui a une importance majeure dans le cadre de la protection des données à caractère personnel.

La communication de ces données doit se faire en langage clair et être conforme aux enregistrements. La directive parle de forme intelligible. Par conséquent le fournisseur d'accès à Internet ou le fournisseur d'hébergement qui est saisi d'une telle demande ne pourra pas donner des fichiers « logs » qui seraient des suites de chiffre ou de lettre compréhensible par lui seul. Il devra communiquer des informations qui permettront à l'internaute de savoir par exemple à quelle heure et à quelle date il s'est connecté et toutes les informations afférentes à cette connexion que détient le fournisseur d'accès.

La loi prévoit que la personne qui exerce ce droit d'accès peut obtenir copie des informations sur imprimante (ou sur support informatique dans la loi à venir)

La remise d'une copie peut être subordonnée au paiement d'une redevance fixée par les textes d'application (20FF pour le secteur public et 30 FF pour le secteurs privé). Il ne peut être demandé une redevance d'un montant supérieur à peine d'une contravention de 3^{ème} classe⁸

Dans la pratique le secteur public a tendance à faire payer afin de dissuader les personnes concernées alors que le secteur privé a tendance à ne pas faire payer car le demandeur est souvent un membre du personnel, un client, un prospect, ... de plus il faudrait mettre en place une structure de paiement ce qui est parfois plus compliqué que de répondre de manière assez rare à des demandes de communication.

La loi prévoit des délais de réponse : la CNIL saisit par le responsable du fichier peut accorder des délais supplémentaires, mais ceci suppose qu'il saisisse la CNIL, et en tout état de cause, ceci ne dispense pas de répondre. Dans la pratique c'est un droit très rarement utilisé.

La loi prévoit que la CNIL peut aller jusqu'à dispenser de réponse le responsable du traitement quand les demandes sont manifestement abusives par leur nombre, leur caractère systématique ou leur répétitivité.

C – Le droit de contestation et d'obtenir rectification des données personnelles le concernant

Ce droit est prévu par l'article 36 de la loi de 1978 et l'article 12 de la directive, il permet de contester les informations que détient le fournisseur d'accès à Internet ou le fournisseur d'hébergement et d'obtenir la rectification de ces données.

Le fait de s'opposer à l'exercice du droit de rectification est sanctionné par une amende de 5^{ème} classe⁹

La demande de rectification peut déboucher sur deux possibilités :

⁸Article 2 du décret du 23 décembre 1981

⁹Decret du 23 décembre 1981

Le responsable accepte la revendication de la personne alors il s'agit d'un arrangement à l'amiable afin de rectifier les données.

Ou bien la demande de rectification débouche sur un conflit : celui qui gère l'information dit que l'information est bonne alors la charge de la preuve incombe au responsable du traitement.

La personne qui a obtenu une modification peut demander copie du nouvel enregistrement modifié, le refus constitue une contravention de 5ème catégorie.

Ce droit d'obtenir la copie est gratuit. Quand il y a eu une modification il faut rembourser la redevance payée au niveau de la copie liée au droit d'accès.

La personne qui a des difficultés à exercer son droit d'accès au sens large a la possibilité de se plaindre directement auprès de la CNIL.

D – Le droit de s'opposer au traitement de données à caractère personnel

Le droit d'opposition est prévu par l'article 26 de la loi de 1978 et l'article 14 de la directive.

Toute personne physique a le droit de s'opposer pour des raisons légitimes à ce que des données nominatives le concernant fassent l'objet d'un traitement. Avant comme pendant, à tout moment, même si l'on a accepté avant. Cependant la loi n'impose pas une information pour dire qu'il existe un droit d'opposition.

Le non respect de ce droit est sanctionné pénalement par 5 ans d'emprisonnement et 300.000 euros d'amende¹⁰

Concernant la notion de « raisons légitimes », il s'agit d'un vocabulaire non juridique, ce sont des raisons sérieuses tenant au demandeur *in concreto*, par conséquent le droit à être laissé tranquille est une raison légitime. La directive de 1995 ajoute « une raison légitime et prépondérante », ce que ne prévoit pas le projet de loi.

Dans certains cas la notion de raison légitime disparaît¹¹ lorsque le droit d'opposition s'applique, en matière de prospection où on peut refuser sur demande gratuitement le traitement envisagé.

¹⁰ Article 226-18 du Code Pénal

La CNIL prévoit aussi cette non-justification pour l'Internet.

Le droit d'opposition ne peut être supprimé que dans le secteur public, pour les traitements automatisés de données.

Les fournisseurs d'accès à Internet et les fournisseurs d'hébergement peuvent donc se voir contraints de ne pas pratiquer de traitement de données à caractère personnel concernant certains de leurs clients qui l'aurait demandé. Cependant il est vraisemblable que les traitements de données à caractère personnel sont indispensables au fonctionnement technique des services proposés par les fournisseurs d'accès à Internet et les fournisseurs d'hébergement, par conséquent le recours au droit d'opposition par le client amènera le prestataire à mettre fin au service qu'il proposait à cette personne.

En pratique donc l'utilisation du droit d'opposition vis à vis d'un fournisseur d'accès à Internet ou un fournisseur d'hébergement est absurde.

E. Le droit de connaître la logique qui sous-tend le traitement

Apparaît dans l'article 3 de la loi de 1978, et dans l'article 12 de la directive de 1995.

Dès 1978, on a prévu un tel droit, c'est un droit intéressant mais qui est celui qui fonctionne le moins dans la pratique, cependant dans le futur il est possible de découvrir des potentialités.

Pour la loi de 1978 et la directive de 1995, ce droit ne concerne que les traitements automatiques et pas les traitements manuels.

L'article 3 dispose que toute personne a le droit de connaître et de contester les informations et les raisonnements utilisés dans les traitements automatisés dont les résultats lui sont opposés.

Articulation entre l'article 3 et l'article 2, l'article 2 prévoit qu'on ne peut pas se fier seulement à la machine pour prendre une décision.

¹¹Article 14 de la Directive de 1995

L'alinéa second concerne les autres décisions (administratives comme privées) impliquant une appréciation sur un comportement humain, celles-ci ne peuvent avoir pour seul fondement un traitement automatisé, cependant les personnes qui utilisent un tel procédé diront toujours que ce n'est pas le seul fondement puisque la décision finale est prise par un humain, mais en pratique la décision prise est la copie conforme de celle prise par le traitement automatisé.

Le contenu de l'article 3 permet de connaître les informations et les raisonnements, l'article reconnaît le droit d'accès à la structure du logiciel d'aide à la décision, la pondération des critères, l'existence même des critères.

Ce droit pourrait être envisagé dans les cas où un traitement automatisé de données à caractère personnel conduirait le fournisseur d'accès à Internet ou le fournisseur d'hébergement à prendre des décisions concernant un internaute.

Ceci peut être le cas pour les fournisseurs d'accès lorsque ceci met fin au contrat de leur abonné pour utilisation excessive de leur connexion comme ce fut le cas avec certains fournisseurs d'accès à Internet gratuits.

Pour les fournisseurs d'hébergement ceci peut concerner les pratiques qui consistent à bannir un utilisateur ou une adresse IP pour des abus.

Dans ces deux cas, il s'agit de procédures automatiques qui pourraient faire l'objet de demande de la part des internautes concernés afin de connaître les critères de ces procédures automatiques.

§2. La protection par le secret

I. L'interdiction d'interception et de conservation

A) Une interdiction de principe

L'article 5 de la directive 97/66/CE garantit la confidentialité des communications, interdisant à tout autre personne que l'utilisateur, sans le consentement de celui-ci, d'écouter, intercepter, stocker les communications ou les soumettre à quelque autre moyen d'interception ou de

surveillance, sauf lorsque ces activités sont légalement autorisées (conformément à l'article 14 paragraphe 1).

Ce régime se traduit par l'obligation d'effacer ou de rendre anonyme les données relatives au trafic dès la fin de la connexion imposée par l'article 6 paragraphe 1.

C'est aussi ce qu'exige la loi de 1986 relative à la liberté de communication.

B) L'exception destinée à la facturation

Cependant l'article 6 (2) de la directive 97/66/CE comme la loi de 1986 pose une exception pour les données destinées à la facturation, pour lesquelles, un traitement est autorisé jusqu'à la fin de la période au cours de laquelle la facture peut être contestée, ou des poursuites engagées afin d'en obtenir le paiement.

Les fournisseurs d'accès à Internet et les fournisseurs d'hébergement peuvent donc conserver les données de connexion de leurs clients afin de facturer leurs services et prouver notamment les dates, les heures, les volumes de connexion.

C) L'exception liée à la recherche d'infractions

Concernant la rétention des données dans le secteur des communications électroniques, la directive 2002/58/CE stipule que les états membres ne peuvent lever la protection des données que pour permettre des enquêtes criminelles ou préserver la sécurité nationale, la défense et la sécurité publique. La directive impose aussi un principe de proportionnalité de la mesure en considérant qu'une telle mesure doit être "nécessaire, appropriée et proportionnée dans une société démocratique"

Il s'agit ici d'une exception qui n'est pas forcément existante, elle permet juste aux autorités qui le souhaitent de mettre en place un tel système.

II. L'interdiction de divulgation

L'interdiction de divulguer les données résulte directement de l'interception de les détenir et de les conserver.

Si la détention des données n'est pas légitime, alors la divulgation n'est pas possible. En effet toute divulgation traduirait une détention illicite et il n'y a donc pas besoin d'interdiction spécifique de divulgation : la divulgation est incluse dans la violation du secret.

Si la détention des données entre dans une des exceptions à l'interdiction, la divulgation est encadrée par des règles spécifiques, liées à l'objet de l'exception elle-même. Dans le cas des données nécessaires à la facturation par exemple, la divulgation ne peut être faite que pour traiter cet unique objectif. Pour ce qui concerne la recherche d'infractions, la divulgation est encadrée notamment par le code de procédure pénale.

Les règles générales relatives aux données à caractère personnel que nous avons vu jusqu'ici sont très protectrices des personnes concernées, elles encadrent au maximum la collecte et l'utilisation des données et tentent d'en limiter les usages abusifs ou attentatoires aux libertés. Cependant, des règles spécifiques concernant les fournisseurs d'accès à Internet et les fournisseurs d'hébergement ont été édictées, et celle-ci aménagent les règles générales pour un régime moins protecteur.

Chapitre 2. Un régime spécial qui aménage les dispositions protectrices

Au delà du régime lié au type même de données concernées, l'activité même de fournisseur d'accès à Internet et de fournisseur d'hébergement place ces prestataires à un point crucial pour appliquer un certain nombre de lois et pour lutter contre la cybercriminalité.

Il en découle un régime spécifique qui se traduit à la fois par une obligation de conservation des données à caractère personnel (Section 1) et par une obligation de divulgation des données à caractère personnel à certaines autorités (Section 2).

Section 1. Les obligations de conserver les données à caractère personnel

Les différentes obligations prévues par les lois spéciales imposent la conservation de données à caractère personnel à la fois au fournisseur d'hébergement (paragraphe 1) et au fournisseur d'accès à Internet (paragraphe 2)

§1. L'obligation du fournisseur d'hébergement

I. Une obligation justifiée par le droit de la presse

Le droit de la presse est marqué par un régime spécifique de responsabilité dit "en cascade" où les différents participants (auteur, imprimeur, éditeur, ...) peuvent être actionnés en responsabilité.

Afin de faciliter la mise en œuvre de ce régime, le droit de la presse impose une identification claire des différents acteurs.

Les sites Internet sont soumis au droit de la presse, par conséquent l'ensemble des dispositions relatives au droit de la presse s'applique, mais au-delà de ces règles générales, le législateur a souhaité créer un régime spécial à destination des sites Internet.

Le fournisseur d'hébergement se trouve à un point stratégique afin de faire respecter les différentes obligations relatives aux sites Internet, puisque c'est lui qui détient, sur ses serveurs, l'ensemble des pages mises à la disposition du public, il est l'intermédiaire entre l'éditeur du contenu et leur destinataire qu'est l'internaute.

II. L'étendue de l'obligation du fournisseur d'hébergement

A) Les données visées

Le fournisseur d'hébergement doit détenir et conserver les données de nature à permettre l'identification de toute personne ayant contribué à la création d'un contenu des services dont il est prestataire. C'est ce que prévoit l'article 43-9 de la loi du 30 septembre 1986 sur la liberté de communication.

Article 43-9 : « Les prestataires mentionnés aux articles 43-7 et 43-8 sont tenus de détenir et de conserver les données de nature à permettre l'identification de toute personne ayant contribué à la création d'un contenu des services dont elles sont prestataires. »

On voit que la loi vise à la fois les fournisseurs d'accès à Internet et les fournisseurs d'hébergement, cependant l'activité visée « la création d'un contenu des services dont elles sont prestataires » vise clairement l'activité d'hébergement. Cependant, ce n'est pas étonnant puisque dans la pratique tous les fournisseurs d'accès fournissent un hébergement à leur client.

La loi prévoit aussi qu'« Ils sont également tenus de fournir aux personnes qui éditent un service de communication en ligne autre que de correspondance privée des moyens techniques permettant à celles-ci de satisfaire aux conditions d'identification prévues à l'article 43-10. »

La loi renvoi en dernier lieu à un décret en Conseil d'Etat, pris après avis de la Commission nationale de l'informatique et des libertés pour définir les données concernées, la durée et les modalités de leur conservation. Malheureusement ce décret n'est toujours pas paru.

B) Durée

La durée doit être précisée par le décret qui est toujours en attente.

Cependant, si on considère la finalité de cette conservation qu'est l'identification des auteurs de contenus hébergés, alors on peut déjà considérer que la durée minimum sera la durée de l'hébergement. A la fin de l'hébergement, le contenu n'étant plus en ligne, la conservation des données d'identification n'est plus justifiée. Elle pourrait être rallongée de quelques mois afin de permettre à une personne qui recherche l'identité d'un site venant de fermer de trouver ces informations auprès du fournisseur d'hébergement.

§2. L'obligation du fournisseur d'accès à Internet

I. Une obligation justifiée par la lutte contre la « cybercriminalité »

Les fournisseurs d'accès à Internet sont les prestataires techniques les mieux placés dans la lutte contre la cybercriminalité en général, en effet, ils sont le maillon indispensable qui relie l'internaute au réseau Internet. Il est exclu d'accéder au réseau Internet sans passer par un fournisseur d'accès à Internet, en dehors d'hypothèses marginales où la personne serait son propre fournisseur d'accès à Internet.

Ce rôle permet au fournisseur d'accès à Internet de voir transiter sur son infrastructure toutes les données permettant de connaître l'activité de ses clients sur Internet.

Au-delà de ces informations qui ne font que transiter et ne peuvent être stockées pour des raisons pratiques et techniques d'infrastructure, le fournisseur d'accès peut conserver certaines données, qui si elles ne sont pas aussi complètes, permettent de fournir des informations aux autorités compétentes afin d'identifier des internautes.

Les fournisseurs d'accès à Internet sont donc les prestataires les plus susceptibles d'être sollicités lors des procédures d'identification d'auteurs de comportements illicites sur Internet. C'est pourquoi afin de se ménager les preuves dans de telles hypothèses, le législateur a souhaité imposer un minimum d'informations que le fournisseur d'accès à Internet est tenu de conserver.

II. L'étendue de l'obligation du fournisseur d'accès à Internet

A) Les données concernées

a) Les types de données

La directive « vie privée et communications électroniques » définit la notion de « données relatives au trafic » comme « les données traitées en vue de l'acheminement d'une communication par un réseau de communications électroniques ou de sa facturation »¹². Il y a donc lors de l'établissement d'une communication électronique deux composantes : la communication elle-même qui en réalité est son contenu et qui pourrait donc être éventuellement assimilé à une correspondance au sens du droit français et les données relatives au trafic qui sont les données techniques indispensables à l'établissement et l'acheminement de la communication.

En effet qu'une communication soit électronique ou non, pour être acheminée elle doit faire apparaître aux intermédiaires chargés de son transport diverses informations. Un courrier papier contient au minimum le nom et l'adresse du destinataire, ainsi que la date et le lieu où le courrier a été posté par l'intermédiaire du cachet de la poste. Il en est de même avec les communications électroniques qui utilisent le réseau Internet dont les données de trafic peuvent contenir l'adresse du destinataire et de l'expéditeur mais aussi des données telles que le chemin pris par le messages (le routage), le volume et la date de la communication, ... toutes ces données techniques sont

¹² Directive 2002/58/CE, article 2.b

utiles pour transmettre efficacement les données mais elles sont aussi des données à caractère personnel.

La notion de « donnée relative au trafic » est assez floue, la terminologie même n'est pas stable, ainsi la loi sur la sécurité quotidienne utilise le terme de « donnée relative à une communication » mais d'autres notions semblent recouvrir la même notion : « données de connexion », « données de trafic », « données de transaction », « données d'identification » selon les auteurs.

Les données de connexion sont des données identifiant à un moment donné le client connecté au réseau et son adresse IP et éventuellement d'autres informations relatives uniquement à la connexion (login, mot de passe). Ces informations permettent avec une adresse IP et une heure de connexion de connaître l'identité de la personne qui détenait l'adresse IP.

Les données de navigation sont en réalité la communication elle-même, c'est à dire le contenu des sites visités, elles ne sont pas nécessaires à l'établissement d'une communication, ce ne sont pas des données techniques mais du pur contenu.

La loi de 1986 prévoit que les données concernées *« portent exclusivement sur l'identification des personnes utilisatrices des services fournis par les opérateurs et sur les caractéristiques techniques des communications assurées par ces derniers. Elles ne peuvent en aucun cas porter sur le contenu des correspondances échangées ou des informations consultées, sous quelque forme que ce soit, dans le cadre de ces communications. »*. Il ne s'agit donc que de conserver les données de connexion à l'exclusion des données de navigation.

Cependant en attendant le décret en conseil d'état relatif a ces données, les notions de données de connexion est encore floue et pourra donner lieu à des interprétations multiples.

b) L'utilisation des données

Le code des postes et télécommunications a été modifié par la loi sur la sécurité quotidienne et prévoit que bien que le principe soit l'effacement ou l'anonymisation des données relatives à une communication, il peut y avoir une conservation dans certains cas :

- *« Pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales, et dans le seul but de permettre, en tant que de besoin, la mise à disposition de*

l'autorité judiciaire d'informations, il peut être différé pour une durée maximale d'un an aux opérations tendant à effacer ou à rendre anonymes certaines catégories de données techniques » Il s'agit ici de permettre l'accès aux données à caractère personnel conservées par les fournisseurs d'accès à Internet par les autorités judiciaires. C'est la raison d'être de cette conservation des données, qui permet ainsi de ménager des preuves dans la recherche d'infractions commises au moyen d'Internet. Concernant les données et la durée de conservation des différentes données la loi renvoi encore à un décret en Conseil d'état, pris après avis de la Commission nationale de l'informatique et des libertés. La loi prévoit ici un possibilité d'indemnisation des fournisseurs d'accès pour cette conservation. Car, en effet, le coût du stockage de ces informations, est très important d'autant que le volume d'informations concerné est impressionnant.

- La loi prévoit aussi une exception en ce qui concerne la facturation, comme pour les fournisseurs d'hébergement, en autorisant les fournisseurs d'accès à Internet « *jusqu'à la fin de la période au cours de laquelle la facture peut être légalement contestée ou des poursuites engagées pour en obtenir le paiement, utiliser, conserver et, le cas échéant, transmettre à des tiers concernés directement par la facturation ou le recouvrement* »
- Comme nous l'avons dit précédemment, le coût du stockage est élevé, et les fournisseurs d'accès à Internet ont été très hostiles à l'établissement d'une obligation de conservation des données à caractère personnel. Le gouvernement, afin d'éviter un conflit, leur a accordé une faveur de taille en leur permettant de « *réaliser un traitement de ces données en vue de commercialiser leurs propres services de télécommunications, si les usagers y consentent expressément et pour une durée déterminée* ». Cette autorisation ne valant que pour la période contractuelle entre le fournisseur d'accès à Internet et son client. Le gouvernement a ici cédé aux intérêts commerciaux des fournisseurs d'accès à Internet au détriment des clients de ceux-ci qui se verront imposer cette utilisation de leurs données à caractère personnel dans les contrats d'hébergements qui sont des contrats d'adhésion où la volonté du client n'a souvent guère d'importance.
- Enfin, la loi prévoit aussi que les fournisseurs d'accès à Internet peuvent conserver certaines données « *en vue d'assurer la sécurité de leurs réseaux* », ici l'autorisation est très vague sans limitation de données, de durée. Ce sera donc au juge de juger de la légitimité pour le fournisseur d'accès à Internet de conserver certaines données, car le texte de la loi laisse libre

cours à tous les abus. Les actualités informatiques concernant les « vers » (les *worms*) le montre, la sécurité du réseau pourrait passer par l'analyse du contenu même des communications, car c'est la seule manière d'arrêter de manière efficace et définitive ces programmes informatiques.

- La loi rappelle que les fournisseurs d'accès sont tenus de prendre toutes les mesures pour empêcher une utilisation des données de connexion à d'autres fins que celles prévues précédemment. Il semble donc, selon les termes de la loi, qu'il s'agisse d'une obligation de moyen à la charge du fournisseur d'accès. Il semble que ce soit en réalité une sorte d'obligation de sécurité comme celle prévue par la loi informatique et libertés qui impose au fournisseur d'accès à Internet d'éviter une utilisation abusive des données par un tiers, car l'obligation n'aurait aucun sens si elle concernait une utilisation par lui-même.
- Enfin, il est très intéressant de voir, que le législateur a tenu à préciser que cette législation n'est pas une zone de remise en cause totale des droits relatifs à la protection des données à caractère personnel puisqu'il a inséré une disposition qui prévoit que « *La conservation et le traitement de ces données s'effectuent dans le respect des dispositions de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.* », il ne s'agit donc qu'un aménagement à la loi de 1978, il était bon de le préciser car cette disposition limite les usages abusifs de ces exceptions, et permettent l'application de règles protectrices à ces fichiers.

B) La durée

a) La discussion sur la durée

1. La pratique de l'Association des fournisseurs d'accès et de services Internet (A.F.A.)

L'association des fournisseurs d'accès s'est exprimée sur le sujet de la durée de conservation des données de connexion à Internet¹³.

En pratique, bien avant la loi sur la sécurité quotidienne, l'Association des fournisseurs d'accès et de services Internet avait édicté pour ses membres une charte relative à la conservation des données à caractère personnel dans laquelle elle recommande une durée de conservation de 3 mois, ce délai ayant été fixé « par la déontologie professionnelle en cohérence avec les recommandations des autorités de protection des données à caractère personnel et la pratique internationale »

L'Association des fournisseurs d'accès et de services Internet recommande donc l'extension de la durée de 3 mois comme la durée de conservation légale des données de connexion.

2. L'avis de la Commission Nationale Informatique et Libertés

La Commission Nationale Informatique et Libertés relevant la nécessité d'une juste proportionnalité entre les différents intérêts en cause et observant les différentes pratiques européennes considère que la durée de 3 mois répondrait à ces impératifs et satisferait les différentes parties concernées.

3. L'avis du forum des droits sur l'Internet

Le forum des droits sur l'Internet recommande « D'adopter une durée de conservation des données de communication différenciée en fonction des données : si les données relatives à la facturation doivent être conservées pendant une année par les opérateurs (du fait du délai de prescription prévu à l'article L.32-3-2 de Code des postes et télécommunications), la durée de conservation des données à des fins d'enquête peut être plus courte. Il paraît, par exemple, difficilement concevable de conserver les données des proxies pendant un an. Le Forum

¹³ Les forum des droits sur l'Internet, 5 novembre 2001 – Forum « Données de connexion »

considère cependant que, du moment que les données à conserver sont définies de manière restrictive et qu'aucun accès général à ces données n'est autorisé, la durée de conservation de ces données, à condition qu'elle n'excède pas une année, doit être dictée par des impératifs d'efficacité de l'action des forces de sécurité. Il rappelle néanmoins que le coût de cette conservation est à la charge de l'Etat. »

4. L'avis de la Brigade d'enquête sur les Fraudes aux Technologies de l'Information

La BEFTI qui est un service dépendant de la Direction Régionale de la Police Judiciaire de Paris a pour mission de lutter contre les atteintes aux systèmes de traitement automatisés d'information, c'est à ce titre qu'elle a donné son avis sur la durée de conservation des données personnelles¹⁴.

Elle fait d'abord plusieurs constatations :

- Le délai entre la commission de l'infraction et la constatation par la victime des faits peut atteindre plusieurs semaines.
- Dans le cas d'une infraction internationale, une commission rogatoire peut prendre plusieurs mois.

Il en résulte selon ses chiffres que 25% des plaintes n'aboutissent pas du seul fait du non stockage des données techniques.

Elle recommande donc une conservation d'une durée d'un an qui semble, à ses yeux, le plus raisonnable.

5. L'avis du groupe de travail de l'article 29

¹⁴ Contribution de la BEFTI au forum « données de connexion », Le forum des droits sur l'internet, 14 novembre 2001.

Le groupe a été établi en vertu de l'article 29 de la directive 95/46/CE. Il s'agit d'un organe consultatif européen indépendant sur la protection des données et de la vie privée.

Il émet régulièrement des avis relatifs à la protection des données.

Dans un avis de 2003¹⁵, le groupe de travail exige une interprétation des directives en vertu du principe de proportionnalité, et considère « *qu'une interprétation raisonnable des directives sur la protection des données implique une période maximale de stockage systématique de 3 à 6 mois pour la facturation* »

Dans une recommandation de 1999¹⁶ le groupe de travail considère « *que le moyen le plus efficace de réduire des risques inacceptables pour la vie privée tout en reconnaissant la nécessité d'une application efficace de la loi voudrait que les données relatives au trafic ne soient pas en principe conservées à des fins de respect de la loi et que les législations nationales n'obligent pas les opérateurs de télécommunications, les fournisseurs de services de télécommunications et de services interne à conserver des données relatives au trafic pendant une période plus longue qu'il n'est nécessaire à des fins de facturation* »

Le groupe de travail considère donc qu'aucune législation spécifique sur la durée de conservation des données de trafic n'est nécessaire, que la simple conservation à des fins de facturations pour une durée de 3 à 6 mois est donc suffisante. Ceci reposant notamment sur le constat que la durée de 3 mois adoptée dans certains pays d'Europe a donné de très bons résultats.

6. Approche de droit comparé : les exemples étrangers

Suisse : La législation suisse¹⁷ impose la conservation des données relatives à l'établissement d'une connexion lors d'une navigation sur Internet et les données touchant à l'échange des

¹⁵ Avis 1/2003 sur le stockage des données relatives au trafic à des fins de facturation, adopté le 29 janvier 2003

¹⁶ Recommandation 3/99 relative à la préservation des données de trafic par les fournisseurs de services Internet pour le respect du droit

¹⁷ Ordonnance du 31 octobre 2001 (admin.ch) sur la surveillance de la correspondance par poste et télécommunication (OSPCT)

courriers électroniques pendant une durée de 6 mois. Le texte permet de verser des indemnités aux fournisseurs d'accès pour compenser le coût engendré par cette obligation de conservation, celle-ci est forfaitaire.

La Commission Nationale Informatique et Libertés relève¹⁸ les différentes pratiques européennes : l'Allemagne, les Pays-Bas et la Finlande pratiquant une durée de 3 mois, la Suisse 6 mois. La majorité des pays européens pratiquant la conservation des données entre 3 et 6 mois. La Tchéquie impose la conservation pendant 2 mois et la Belgique pendant un an.

b) La durée adoptée

Lors de la discussion sur la loi sur la sécurité quotidienne, le législateur a par voie d'amendement porté la durée de conservation des données de connexion par les fournisseurs d'accès de trois mois à un an.

On voit donc qu'à l'origine, le projet de loi prévoyait une durée de conservation alignée avec les souhaits des prestataires, des associations, ... mais les législateurs en ont décidé autrement.

La durée d'un an semble respecter par les fournisseurs d'accès puisque le tribunal d'instance de Vanves¹⁹ a constaté que les données relatives à la création d'un compte chez le fournisseur d'accès à Internet Wanadoo avait été détruites, « destruction permise dans le délai d'un an » et qu'ainsi il n'avait pas à communiquer l'identité du créateur du compte Internet.

Section 2. Les obligations de divulguer les données à caractère personnel

Les données à caractère personnel ainsi conservées n'ont de raison d'être que si elles peuvent être divulguées, cette divulgation peut avoir lieu actuellement dans le cadre des réquisitions

¹⁸ Forum des droits de l'Internet, 5 novembre 2001 – Forum « Données de connexion »

¹⁹ Tribunal d'instance de Vanves, Ordonnance de référé du 25 juin 2002, Alain D. contre Société Wanadoo Interactive, Société Intrum Justifia

judiciaires (paragraphe 1) mais un nouveau régime est en train de se développer avec les textes à venir (paragraphe 2)

§1. Les réquisitions judiciaires

I. Une obligation générale

Avant même l'adoption d'une loi particulière, il a toujours été possible de réclamer dans le cadre d'une procédure judiciaire les données relatives à l'identification des auteurs d'infractions.

Ceci se base sur différents textes :

L'article 10 du Code Civil qui dispose que chacun est tenu d'apporter son concours à la justice en vue de la manifestation de la vérité. C'est le fondement utilisé par le tribunal de commerce de Paris²⁰ pour imposer la communication par le fournisseur d'hébergement de l'identité du créateur d'un site litigieux, le juge va même jusqu'à considérer qu'en temps que fournisseur d'hébergement « il se doit d'avoir conservé les journaux des connexions FTP du site hébergé »

L'article 145 du nouveau code de procédure civile permet lorsqu'il existe un motif légitime de conserver ou d'établir avant tout procès la preuve des faits dont pourrait dépendre la solution d'un litige de demander au juge sur requête ou en référé d'ordonner les mesures d'instructions légalement admissibles. C'est sur ce fondement que le tribunal de grande instance de Paris²¹ a justifié son ordre à un fournisseur d'accès à Internet de communiquer l'identité d'un utilisateur à partir de la date, l'heure et l'adresse IP de celui-ci. Ce texte est encore invoqué à titre subsidiaire²² des textes modifiés par la loi du premier août 2000.

²⁰ Tribunal de Commerce de Paris, Ordonnance de référé du 29 juin 2000 : Société Nationale de Radiodiffusion Radio France contre Monsieur Valentin Lacambre.

²¹ Tribunal de Grande Instance de Paris, Ordonnance de Référé 1 février 2002, SPPI contre T-Online France

²² Tribunal de Grande instance de Paris, Ordonnance de référé, 31 mai 2002, Gandi SARL

On voit donc que les dispositions de droit commun permettaient déjà d'exiger des fournisseurs d'accès à Internet et des fournisseurs d'hébergement la communication des données d'identification en leur possession. Mais cette obligation a été explicitée pour le cas spécifique des fournisseurs d'accès à Internet et des fournisseurs d'hébergement.

II. Une obligation renforcée par la loi du premier août 2000

La LSQ a introduit un article 43-9 dans la loi de 1986 qui dans son alinéa 3 dispose « Les autorités judiciaires peuvent requérir communication auprès des prestataires mentionnés aux articles 43-7 et 43-8 des données mentionnées au premier alinéa. Les dispositions des articles 226-17, 226-21 et 226-22 du code pénal sont applicables au traitement de ces données. »

La loi relative à la sécurité quotidienne²³ a aussi introduit un nouvel article L. 32-3-1 dans le code des postes et télécommunications.

Cette loi malgré un premier alinéa qui énonce le principe de d'effacement et d'anonymisation, remet clairement ce principe en cause en permettant aux autorités judiciaires d'obtenir l'identité des internautes pendant une année au maximum.

Afin de s'assurer de la conservation effective de ces données par les prestataires, la loi a intégré deux avantages de nature économique à l'attention de ces opérateurs :

- La loi relative à la sécurité quotidienne a tout d'abord introduit une atténuation de taille à la loi informatique et libertés en autorisant les opérateurs à utiliser ces données à des fins commerciales. Certes cette utilisation est encadrée par l'article L. 32-3-1.III alinéa 2 des codes des postes et télécommunications qui prévoit que ce traitement ne peut être effectué par les opérateurs qu'afin de « *commercialiser leurs propres services de télécommunications, si les usagers y consentent expressément et pour une durée déterminée* ». Cependant, il s'agit d'une exception à l'un des principes fondamentaux de la loi informatique et libertés qu'est le principe de finalité.

- Ensuite, la loi relative à la sécurité quotidienne prévoit l'éventualité d'une compensation financière. Cette éventualité est laissée au domaine du décret qui devra donc déterminer « *les modalités de compensation, le cas échéant, des surcoûts identifiables et spécifiques des prestations assurées à ce titre, à la demande de l'état, par les opérateurs* »

Le législateur a donc intégré dans cette loi, à l'occasion d'un mouvement mondial de lutte contre le terrorisme, des dispositions qui remettent sérieusement en cause le principe de secret et de non-conservation des données à caractère personnel. Afin de limiter l'hostilité des prestataires techniques à ces nouvelles obligations, il a intégré un double dispositif d'indemnisation économique. Le secteur associatif est très mobilisé à l'encontre de ce texte. Mais leur mobilisation est d'autant plus forte que des textes à l'étude suivent cette voie.

§2. Les textes à venir

Des textes à venir pourraient venir compléter ce régime juridique relatif aux fournisseurs d'accès à Internet, aux fournisseurs d'hébergement et aux données à caractère personnel, il s'agit de loi sur l'économie numérique et la nouvelle loi « informatique et libertés ».

I. Le projet de loi sur l'économie numérique (Ancienne L.S.I.)

Le projet de loi sur l'économie numérique remplace le projet de loi sur la société de l'information du gouvernement précédent, bien qu'il ne recouvre pas exactement le contenu de ce dernier. Ce projet de loi vise aussi à transposer la directive du 8 juin 2000 qui aurait du être transposée avant le 17 janvier 2002. Le projet de loi sur la confiance en l'économie numérique va transposer les dispositions de la directive 2002/58 alors que la directive 95/46 n'a toujours pas été transposée.

Le projet de loi sur l'économie numérique renouvelle l'obligation faite aux prestataires intermédiaires de conserver les données d'identification en revoyant à un décret qui est attendu

²³Loi du 15 novembre 2001 « relative à la sécurité quotidienne »

depuis le 1^{er} août 2000.. Le projet de loi dispose que la loi de 1986 sera modifiée en prevoyant dans son aricle 43-13 : « Les personnes mentionnées aux articles 43-7 et 43-8 sont tenues de détenir et de conserver les données de nature à permettre l'identification de quiconque a contribué à la création du contenu ou de l'un des contenus des services dont elles sont prestataires. Elles sont également tenues de fournir aux personnes qui éditent un service de communication publique en ligne des moyens techniques permettant à celles-ci de satisfaire aux conditions d'identification prévues à l'article 43-14. »

Elle confirme donc l'obligation de détention et de conservation des données à caractère personnel relatif aux auteurs des contenus hébergés par ses soins. Et impose aussi une obligation de conseil et de fourniture de moyens relatifs à cette identification. Par conséquent on risque de voir des actions à la fois contre les editeurs de sites et contre leurs fournisseurs d'hébergement en l'absence d'identification des auteurs des sites. Voir meme des actions des editeurs contre leurs fournisseurs d'hébergement qui ne leur auraient pas fourni les moyens techniques d'identification.

Le projet de loi rappelle aussi que l'autorité judiciaire peut requérir communication de ces données auprès des fournisseurs d'accès à Internet et des fournisseurs d'hébergement.

Le projet de loi renvoi à un décret en Conseil d'état, pris après avis de la Commission nationale de l'informatique et des libertés pour définir les données concernées, la durée et les modalités de leur conservation. Un tel décret est attendu depuis la loi sur la sécurité quotidienne de 2000 et n'a toujours pas été publié, on peut espérer que ce décret soit publié après l'adoption de ce projet de loi.

Le projet de loi rappelle les données d'identification que les fournisseurs d'hébergement doivent tenir à la disposition du public :

- s'il s'agit de personnes physiques, leurs nom, prénom et domicile et s'il s'agit de personnes morales, leur dénomination ou leur raison sociale et leur siège social ainsi que s'il s'agit d'entreprises assujetties aux formalités d'inscription au registre du commerce et des sociétés ou au répertoire des métiers, le numéro de leur inscription, leur capital social, l'adresse de leur siège social ;
- Le nom du directeur ou du codirecteur de la publication et, le cas échéant, celui du responsable de la rédaction

- Le nom, la dénomination ou la raison sociale et l'adresse du fournisseur d'hébergement
- Les personnes éditant à titre non professionnel un service de communication publique en ligne peuvent ne tenir à la disposition du public, pour préserver leur anonymat, que le nom, la dénomination ou la raison sociale et l'adresse du fournisseur d'hébergement à condition de lui avoir fourni les éléments d'identification

II. Le projet de modification de la loi Informatique et Libertés

Le parlement est actuellement à l'étude d'un projet de loi modifiant la loi informatique et libertés et notamment destiné à transposer les différentes directives européennes sur le sujet.

La nouvelle loi va pratiquer une uniformisation terminologique en abandonnant la notion d'« information nominative » et en adoptant la terminologie qui est celle de la directive et des autres conventions sur le sujet de « donnée à caractère personnel »

La nouvelle loi adopte le principe de consentement préalable prévu par la directive en exigeant qu'« un traitement de données à caractère personnel doit, soit avoir reçu le consentement de la ou des personnes concernées » . Cette obligation peut paraître extrêmement sévère pour les responsables de traitements. Pour un fournisseur d'accès à Internet la solution sera d'introduire dans le contrat de fourniture d'accès, mais pour un fournisseur d'hébergement il faudrait obtenir l'accord de la personne qui visite un site avant de traiter ses données, soit une procédure très compliquée.

Cependant la directive comme le projet de loi prévoient de nombreuses exceptions si le traitement est nécessaire : « Au respect d'une obligation légale à laquelle le responsable du traitement est soumis », « à la sauvegarde de la vie de la ou des personnes concernées », « à l'exécution d'une mission de service public dont est investi le responsable ou le destinataire du traitement », « à l'exécution, soit d'un contrat auquel la personne concernée est partie, soit de mesures précontractuelles prises à la demande de celle-ci », « à la réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le destinataire, à condition de ne pas méconnaître l'intérêt ou les droits et libertés fondamentaux de la personne concernée. ».

Cette dernière exception semble ruiner totalement le principe de consentement préalable car il y a toujours un intérêt légitime du responsable du traitement à pratiquer ce traitement.

On voit donc qu'*a priori* le projet de loi ne fait que transposer la directive qui elle même était déjà très proche de la loi informatique et libertés de 1978 . Cependant en fonction de l'interprétation donnée par les jurisprudences nationales et européennes à la notion d' « intérêt légitime » on pourra se trouver dans un cas où l'obligation d'un consentement préalable devra s'imposer, cette obligation ne concernera pas le fournisseur d'accès à Internet qui pourra bénéficier de l'exception relative à l'exécution d'un contrat, alors que le fournisseurs d'hébergement ne pourra pas faire valoir cette exception de manière générale vis à vis des internautes visitants les sites hébergés sur ses serveurs.

Bibliographie

A – Textes

1 – Textes Français

- Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.
- La loi de 1986 relative à la liberté de communication
- Loi n°91-646 du 10 juillet 1991.

2 – Textes Européens

- Directive 95/46/CE 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.
- Directive 97/66/CE du 15 décembre 1997 relative au traitement des données à caractère personnel et à la protection de la vie privée dans le secteur des télécommunications.
- Recommandation n° R (83) 10 du Comité des ministres du Conseil de l'Europe sur la protection des données à caractères personnel utilisées à des fins de recherche scientifique et de statistiques, 1983
- La directive 2002/58 du 12 Juillet 2002 « concernant le traitement des données à caractère personnelles et la protection de la vie privé dans le secteur des communications électroniques » dite « vie privée et communication électroniques »
- La charte des droits fondamentaux de l'union européenne adoptée le 7 décembre
- Convention 108 du 28 janvier 1981 relative à la protection des personnes à l'égard du traitement automatisé des données à caractère personnelles.

3 – Textes Internationaux

- L'accord du 15/04/1994 de l'Organisation Mondiale du Commerce

B – Etudes, rapports et colloques

- La directive 97/66/CE du 15 décembre 1997 concernant le traitement de données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications, Aurélie Garcin, Mémoire de DEA Informatique et Droit sous la direction du Professeur Jean Frayssinet, Université Montpellier 1, ERID 1999/2000.
- La transposition de la directive du 24 octobre 1995 relative à la protection des données à caractère personnel et à la libre circulation de ces données : étude européenne, Joelle De Kermadec et Geert Van Grieken, Mémoire de DEA Informatique et Droit sous la direction du Professeur Jean Frayssinet, Université Montpellier 1, ERID 2000/2001.
- L'Internet et le Droit, droit français, européen et comparé de l'Internet, Actes du colloque organisé par l'école doctorale de droit public et de droit fiscal de l'Université Paris I, les 25 et 26 septembre 2000, Collection Legipresse, 2001.
- Les libertés individuelles à l'épreuve des NTIC, Etudes réunies sous la direction de Marie-Christine Piatti, Presses universitaires de Lyon, 2001.

C – Ouvrages

- Lamy Droit de l'Informatique et des Réseaux, sous la responsabilité de Michel Vivant, Edition 2002
- Rapp. L., Le courrier électronique, PUF, 1998, Que sais-je?, n°3409, p.89.

D – Sites Internet

- Forum des droits sur l'internet : <http://www.foruminternet.org/>
- Legifrance : www.legifrance.gouv.fr
- Legalis : www.legalis.net
- Jurisdata : www.juris-classeur.com
- Les Petites Affiches : www.petites-affiches.com

- Droit et Nouvelles Technologies : www.droit-technologie.org
- Droit-NTIC : www.droit-ntic.com
- L'action de l'état pour le développement de la société de l'information :
www.internet.gouv.fr

