Présente :

L'accès aux données de connexion de l'internaute

Mémoire de DEA Droit des Creations Immatérielles

Par

Laurent Teyssandier
Sous la direction de Monsieur le professeur jean Frayssinet

Date de mise en ligne : 27 septembre 2004

UNIVERSITE DE MONTPELLIER I

Faculté de Droit

Année 2004

N° attribué par la bibliothèque

□□□□□□□□

MEMOIRE DE
DEA DROIT DES CREATIONS IMMATERIELLES

Sous la direction de

Monsieur le Professeur Jean Frayssinet

L'ACCES AUX DONNEES DE CONNEXION DE L'INTERNAUTE

Présenté par :

TEYSSANDIER Laurent

E.R.C.I.M.

L'ACCES AUX DONNEES DE CONNEXION DE L'INTERNAUTE

Données de connexion de l'internaute – Définition – Accès – Accès par l'internaute – Accès par des tiers.

Data of connection of the Net surfer - Definition - Access - Access by the Net surfer - Access by thirds

Remerciements

A Monsieur le professeur Jean Frayssinet, pour ses conseils avisés,
et surtout pour la présence, l'attention et la disponibilité
qu'il a su m'accorder tout au long de cette année

A Monsieur le professeur Michel Vivant, pour son sens de la pédagogie
et son ouverture d'esprit, et également pour m'avoir permis
de passer une année riche d'enseignements

A mes parents, pour l'aide et le soutien qu'ils ont su m'apporter chaque jour,
autant dans ma vie personnelle que dans mes études

A mon frère, pour sa joie et sa bonne humeur

A Stéphanie, pour m'avoir toujours encouragé dans mes choix
et pour les moments que nous partageons ensemble
depuis notre rencontre

Et enfin à tous mes amis pour leur aide et l'amitié qu'ils me
Portent chaque jour

SOMMAIRE

INTRODUCTION

« *De tous les carrefours importants, le visage à la moustache noire vous fixait du regard. Il y en avait un sur le mur d'en face. BIG BROTHER VOUS REGARDE, répétait la légende, tandis que le regard des yeux noirs pénétrait les yeux de Winston... Au loin, un hélicoptère glissa entre les toits, plana un moment, telle une mouche bleue, puis repartit comme une flèche, dans un vol courbe. C'était une patrouille qui venait mettre le nez aux fenêtres des gens. Mais les patrouilles n'avaient pas d'importance. Seule comptait la Police de la Pensée*. »

George Orwell, 1984

1. De *1984*[1] à *Brazil*[2], en passant par *The Matrix*[3], la surveillance, le fichage et le contrôle des individus est un des thèmes majeurs du cinéma et de la littérature. On peut ainsi trouver une certaine similitude à ces personnages qui tentent de fuir un monde dans lequel le moindre fait peut être enregistré, analysé puis retourné contre soi. Ainsi, dans *Brazil*, Sam Lowry, fonctionnaire modèle du ministère de l'information nouvellement promu au ministère du recoupement suite à un « bogue » tente de fuir le monde bureaucratique qui l'entoure afin de retrouver la jeune femme qu'il voit dans ses rêves. Dans *The Matrix*, Thomas Andersen découvre que le monde dans lequel il évolue est en réalité élaboré par des machines qui se nourrissent de l'énergie humaine. Le héros tentera alors par tous les moyens d'échapper à un monde dans lequel ses faits et gestes sont constamment épiés par la matrice. Dans tous ces univers, la règle du jeu est la même : surveillance et contrôle de manière continue des individus, fichage et recoupement des informations les concernant… Ces œuvres ne sont que des exemples[4] d'un courant artistique, et

[1] Orwell, G. *1984*. Gallimard

[2] Film de Terry Gilliam, sorti sur les écrans français en 1985

[3] Film de Andy et Larry Wachowski, sorti sur les écrans français en 1999 et suivi de *The Matrix Reloaded* (2003) et *The Matrix Revolutions* (2003)

[4] Voir aussi *Le Meilleur des Mondes*, livre de Aldous Huxley, *Le Procès*, livre de Franz Kafka, *Dark City*, film de Alex Proyas sorti en 1998, ou encore *The Minority Report*, film de Steven Spielberg sorti en 2002…

le sujet du contrôle des citoyens a toujours fortement inspiré les auteurs, notamment de science-fiction. Le plus souvent, ces auteurs imaginent donc un monde dans lequel une autorité supérieure, gouvernement ou entreprise multinationale, opère une surveillance des faits et gestes des individus et un contrôle de leurs pensées et opinions. Pour réaliser ce projet, l'autorité supérieure procède à un fichage total des personnes, de leurs goûts, de leurs opinions, de leurs fréquentations, de leur mode de vie…

2. Sans aller aussi loin que les scénarii catastrophes issus de l'imagination fertile des auteurs de science fiction, force est de constater qu'aujourd'hui les avancées technologiques ont donné les moyens matériels de procéder à une telle surveillance des individus. En effet, l'informatique permet aujourd'hui de pratiquer une surveillance efficace sur un grand nombre de personnes : l'employeur peut surveiller ses salariés, un prestataire technique peut surveiller ses clients sur un réseau[5]… Cependant, il serait faux de penser que cette possibilité est venue de pair avec l'avènement de l'informatique et la démocratisation de l'Internet. Les moyens de contrôle peuvent également se faire sur des techniques plus anciennes, comme le téléphone ou encore le minitel, mais aussi le courrier classique. Certaines personnes peuvent être très intéressées de savoir avec qui nous entretenons des correspondances. Ainsi l'affaire des écoutes téléphoniques survenues entre 1985 et 1986 illustre parfaitement cet intérêt. Ces écoutes étaient menées par la cellule des gendarmes de l'Elysée et visaient des personnes qui avaient déplu à la présidence…

Mais plus encore, il n'a pas fallu attendre l'essor des moyens de télécommunication pour voir se multiplier des tentatives de fichage et de surveillance des individus. La création en 1978 de la Commission nationale de l'informatique et des libertés, autorité administrative indépendante, a fait suite à l'échec d'une tentative de fichage des citoyens français : le projet S.A.F.A.R.I. Ce projet du gouvernement français consistait à organiser l'interconnexion des fichiers nominatifs de l'administration (fiscaux et autres) au moyen du numéro d'identification des individus au répertoire national (N.I.R.) généré par l'Institut national de la statistique et des études

[5] Réseau : Définition publiée par la Commission de l'informatique et des composants électroniques le 10 octobre 1998 : Ensemble des moyens matériels et logiciels mis en oeuvre pour assurer les communications entre ordinateurs, stations de travail et terminaux informatiques.
Équivalent étranger : computer network

économiques. Ce projet était tenu secret mais la presse en eut connaissance et titra « S.A.F.A.R.I. ou la chasse aux Français »[6], ce qui provoqua un fort mécontentement de la population. Le projet fut donc avorté et ce fut la mise en place de la législation sur la protection des informations nominatives et la création de la C.N.I.L. avec la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. Aujourd'hui, il semble que le projet S.A.F.A.R.I. ait été mis en place dans certains secteurs comme dans le domaine fiscal avec la loi de finance de 1999 qui organise l'interconnexion des fichiers sociaux et fiscaux[7].

La justice a elle aussi grand intérêt à procéder à un contrôle continuel des personnes : la constatation des infractions en serait grandement facilitée, puisque l'autorité judiciaire aurait un regard de chaque instant sur les actions des individus.

L'autorité publique n'est pas la seule à vouloir un fichier des individus, certaines entreprises peuvent également y avoir un grand intérêt. De tels fichiers pourraient leur permettre de surveiller non seulement leurs clients mais également leurs concurrents. Ainsi une entreprise pourrait connaître les goûts et les orientations de chaque individu et pourraient donc leur proposer le produit le mieux approprié à leur consommation et à leur mode de vie. C'est là le rêve de tout directeur du serveur marketing et communication d'une entreprise : pouvoir cibler ses offres.

3. Si de telles intrusions étaient réalisées dans la vie des citoyens, nul ne doute qu'elles heurteraient de plein fouet leur droit à la vie privée, et ce, même dans des buts honorables tels que celui de la sauvegarde de la justice. Il y a ici confrontation entre deux intérêts : la sauvegarde de la justice et la sauvegarde de la vie privée et il semble, pour certains, nécessaire que la vie privée doit primer sur la recherche des auteurs d'infractions. Ce sont les droits et libertés fondamentaux des individus qui sont en jeu dans les fichiers comme le rappelle la loi du 6 janvier 1978 dans son premier article « *L'informatique doit être au service de chaque citoyen. Son développement doit s'opérer dans le cadre de la coopération internationale. Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques* ». La vie privée et les droits et libertés fondamentaux des personnes

[6] *Le Monde*, édition du 21 mars 1974

[7] Voir le site Internet des Big Brother Awards à l'adresse <*http://www.bigbrotherawards.eu.org*> qui récompense chaque année les atteintes les plus flagrantes à la vie privée des citoyens.

sont protégés par de nombreux textes nationaux et internationaux. En France, le bloc de constitutionnalité comprend la Déclaration des droits de l'Homme et du citoyen de 1789 qui protège la vie privée à travers la notion de liberté personnelle. Ce principe a été consacré par le Conseil constitutionnel dans une décision du 23 juillet 1999 « Couverture maladie universelle ». Au niveau européen, l'article 8 de la Convention européenne de sauvegarde des droits de l'Homme protège la vie privée et l'article 6 du traité UE dispose que l'union est fondée sur le respect des droits de l'Homme et des libertés fondamentales et fait référence à la convention européenne de sauvegarde des droits de l'Homme. La protection de la vie privée et des droits et libertés fondamentaux de la personne est donc un principe à valeur juridique forte.

4. La surveillance des personnes ne peut se faire que si un fichage est effectué. En effet, comment surveiller une personne si elle est anonyme ? Le fichage pourra donc se faire soit préalablement à la surveillance, soit postérieurement. Le fichage sera postérieur dans le cadre de la vidéosurveillance par exemple : le matériel capturera l'image des personnes, et ensuite au besoin il y aura une identification. Le fichage sera préalable lorsqu'il sera nécessaire de collecter des informations sur les personnes fichées. Ces informations peuvent être de toutes natures : données de connexion à un service de télécommunication, informations personnelles telles que l'état civil ou le numéro d'identification au répertoire, données bancaires pour suivre les variations sur un compte donné… Les fichiers sont nombreux et aujourd'hui nous en voyons de nouveaux se constituer notamment ceux concernant les services de télécommunications. Pour bénéficier d'un service de télécommunication, l'utilisateur dispose souvent d'un terminal servant à se connecter à celui-ci. Ce terminal peut être un téléphone mobile ou fixe, un fax ou un ordinateur[8], mais aussi un GPS qui est un système de positionnement[9]… Sans que leur utilisateur

[8] Ordinateur : Définition publiée par l'arrêté du 30 décembre 1983 : Équipement informatique de traitement automatique de données comprenant les organes nécessaires à son fonctionnement autonome.

Équivalent étranger : computer

[9] Plus exactement GPS signifie Global Positioning System (système de positionnement mondial) et consiste en un Système de radiorepérage qui détermine la position d'un véhicule ou d'un appareil mobile, en se servant d'une constellation de satellites en orbite autour de la Terre. Le système mondial de positionnement est une application civile du système de repérage NAVSTAR (Navigation System using Time and Ranging) mis au point par l'armée américaine. Les signaux émis par les satellites, au nombre de 24, sont captés par un appareil récepteur installé dans

le sache toujours, ces appareils permettent de savoir très précisément ce qu'il fait et où il se trouve. En effet, lorsque l'utilisateur se connecte au service, son terminal doit émettre des données pour la connexion[10]. Par exemple, lorsque l'on allume un téléphone cellulaire, l'appareil se connecte au réseau et envoie donc des données relatives à l'abonnement et des données relatives à la personne de l'abonné. Ces données de connexion sont traitées par le serveur de l'opérateur téléphonique qui sait où est située la personne, qui elle appelle et pour combien de temps. Le principe est le même pour le téléphone filaire, pour le GPS et pour l'ordinateur. L'accès à ces données par des personnes n'ayant pas qualité pour les recevoir constituerait une atteinte certaine à la vie privée et aux droits et libertés fondamentaux de la personne utilisatrice.

5. Les données de connexion posent de grands problèmes dans le secteur de l'informatique et des réseaux. Depuis quelques années, s'est développé Internet[11] qui est un réseau mondial. Les ordinateurs connectés à Internet permettent à leurs utilisateurs d'accéder à un contenu d'une diversité et d'une taille exceptionnelle : il est possible de consulter des informations journalistiques en direct, à des informations culturelles, à de la musique, à des fichiers vidéos… Internet permet également beaucoup d'autres choses : discussions en ligne, messagerie électronique… Les utilisateurs d'Internet, que l'on appelle internautes ou cybernautes, ont donc

---

un mobile. Le système détermine par triangulation la position du mobile, à l'aide de données géographiques informatisées, en fonction du temps et de la distance parcourue par un des satellites en orbite. Définition du Journal du Net, consultable à l'adresse < *http://encyclopedie.journaldunet.com*>

[10] Connexion : Définition publiée par la Commission de l'informatique et des composants électroniques le 10 octobre 1998: Procédure permettant à un utilisateur de se mettre en relation avec un système informatique et, si nécessaire, de se faire reconnaître de celui-ci.

Équivalent étranger : log in, log on

[11] Internet : Définition publiée par la Commission des télécommunications le 16 mars 1999 : Réseau mondial associant des ressources de télécommunication et des ordinateurs serveurs et clients, destiné à l'échange de messages électroniques, d'informations multimédias et de fichiers. Il fonctionne en utilisant un protocole commun qui permet l'acheminement de proche en proche de messages découpés en paquets indépendants. L'acheminement est fondé sur le protocole IP (Internet Protocol), spécifié par l'Internet Society (ISOC). L'accès au réseau est ouvert à tout utilisateur ayant obtenu une adresse auprès d'un organisme accrédité. La gestion est décentralisée en réseaux interconnectés.

Équivalent étranger : Internet network

Forme abrégée : Internet, Net

de grandes possibilités d'exploration grâce à cet outil. Cependant, les données de connexion de l'internaute peuvent causer de graves atteintes à sa vie privée, lorsqu'elles seront interceptées par des personnes malveillantes. Ici revient l'appréhension d'un fichage des individus, rendu aisé par la technique. Il est très facile pour certaines personnes, autorités publiques ou entreprises de créer des fichiers des données de connexion des internautes, données qui permettront de connaître les voyages virtuels de ceux-ci sur le réseau.

Pour ficher les internautes, les personnes devront donc accéder à leurs données de connexion. Si certains accès peuvent être frauduleux, d'autres seront en revanche pleinement autorisés par la loi.

6. Les données de connexion de l'internaute entraînent donc de grandes interrogations notamment sur l'accès même à ces données : qui a accès aux données de connexion de l'internaute, par quels moyens et pour quel objectif ?

Dans le but de répondre à cette interrogation, il conviendra de déterminer auparavant ce qu'est une donnée de connexion car il n'en existe pas de définition.

La première partie sera donc consacrée à la détermination de la catégorie des données de connexion. Afin d'élaborer cette catégorie, nous analyserons toutes les données techniques susceptibles d'y entrer. De cette définition va naître une autre problématique : il faut savoir à qui se rapporte ces données de connexion, autrement dit il faudra délimiter la personne de l'internaute, qui est seulement défini comme tout utilisateur d'Internet par la Commission de l'informatique et des composants électroniques[12].

Une fois les définitions posées, il conviendra d'étudier l'accès à ces données sous deux angles : d'une part l'accès de l'internaute à des données de connexion et d'autre part l'accès aux données de connexion de l'internaute par des tiers.

[12] Définition publiée le 16 mars 1999

La seconde partie sera donc consacrée à l'accès aux données de connexion par l'internaute. Ces données de connexion pourront être celles le concernant mais également celles de tiers. En effet, l'internaute peut vouloir accéder à des données de connexion pour deux raisons : le cybernaute pourra vouloir accéder aux données de connexion le concernant afin de savoir si une atteinte à ses droits est commise. Cet accès pourra se faire par différents moyens que nous étudierons dans un premier temps. Mais l'internaute pourra aussi vouloir accéder aux données de connexion des tiers lorsqu'il subira des atteintes sur Internet, et nous étudierons donc quelles sont ces atteintes et les moyens de s'en protéger dans un second temps. Nous pouvons d'ores et déjà dire que l'une des ces atteintes est l'accès aux données de connexion de l'internaute de manière illicite.

La troisième et dernière partie sera dévolue à l'accès aux données de connexion de l'internaute par des tiers. Ici seront étudiés les accès légaux et licites, les accès illicites ayant été étudiés dans la seconde partie. Les accès licites seront ceux effectués en accord avec la législation, notamment celle protégeant les données à caractère personnel. Enfin seront étudiés les accès judiciaires, lorsque les autorités devront accéder aux données de connexion de l'internaute afin de faire réparer un préjudice ou afin de faire cesser une atteinte à la sécurité publique.

Partie 1. La difficile qualification des données de connexion de l'internaute

7. La doctrine s'est peu penchée sur la question de la détermination des données de connexion de l'internaute. La difficulté de donner une définition claire et précise de ces informations est réelle, tant au niveau de la donnée de connexion en elle-même, qu'au niveau de la personnalisation de l'internaute.

Concernant la donnée de connexion, la profusion et l'hétérogénéité des informations émises lors des connexions au réseau Internet font qu'il est peu évident d'établir une catégorie « donnée de connexion ». Toutefois, nous tenterons d'établir cette catégorie en étudiant les données susceptibles d'être transmises sur l'Internet (chapitre 1).

Concernant l'internaute, c'est entre deux conceptions de sa personne qu'il faudra trancher : entre la conception restrictive de l'internaute comme abonné au service, et la conception expansive de l'internaute comme utilisateur de l'Internet. Là encore, nous tenterons de donner une solution satisfaisante compte tenu des situations rencontrées en pratique (chapitre 2).

Chapitre 1. Les données de connexion : des données hétérogènes

8. La donnée de connexion, si elle n'est pas définie de manière précise, doit comporter certaines caractéristiques. Le site Internet de l'association des fournisseurs d'accès (http://www.afa-france.com) envisage certaines données comme étant des données de connexion. Ces données permettent en premier lieu la connexion de l'internaute au service. Cependant, nous pouvons considérer qu'il ne faut pas borner la donnée de connexion à ce seul usage et qu'il faut l'envisager comme étant plus généralement la donnée qui atteste de la connexion de l'internaute au réseau. Ainsi la donnée de connexion aurait un champ plus large que celui des données permettant la connexion. Cela nous amène donc à nous demander quelles sont les données qui certifient qu'un internaute est connecté.

Lorsque l'internaute se trouve sur le réseau mondial, il émet et reçoit une grande quantité d'informations, que ce soit lors de sa navigation sur la toile, lors de la consultation et l'envoi de courriers électroniques ou encore lors de séances de *chat*[13]. La question que nous pouvons nous poser est celle de savoir si ces données doivent toutes être reconnues comme étant des données de connexion. D'ores et déjà, nous pouvons répondre que toutes ne seront pas à prendre en considération, et il semble acquis que nous ferons face à des difficultés de choix quant aux données qui devront être appréhendées et celles qui devront être rejetées.

Aussi il apparaît difficile de donner une définition précise et concise de la notion de donnée de connexion, tant celle-ci revêt des aspects divers et variés. Pour reprendre la formule du

---

[13] Selon la C.N.I.L., le chat « *correspond à la possibilité de discuter en ligne sur Internet en temps réel avec une ou plusieurs personnes. Contrairement au logiciel de messagerie, le chat permet à l'interlocuteur de prendre instantanément connaissance du contenu du message au moment même où ce dernier est écrit. Afin de pouvoir « chater », il est nécessaire de posséder le logiciel adéquat ou de passer par des sites proposant ce service.* » <www.cnil.fr>

Chat : Définition de la Commission de l'informatique et des composants électroniques publiée le 16 mars 1999 : Communication informelle entre plusieurs personnes sur l'Internet, par échange de messages affichés sur leurs écrans.

Professeur Michel Vivant lorsqu'il définit la propriété intellectuelle, nous pouvons dire que la donnée de connexion est une *notion à géométrie variable*. Cette difficulté à apporter une définition se retrouve aussi dans les textes traitant de ce type de données : certaines lois vont alors envisager les données relatives à la communication (article 29 de la loi n° 2001-1062 relative à la sécurité quotidienne du 15 novembre 2001), d'autres directives vont parler de données relatives au trafic et de données de localisation (article 2b et 2c de la directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002)… Il ressort de ces quelques exemples que la notion de donnée de connexion n'est aujourd'hui qu'une appellation parmi d'autres, et qu'il convient de clairement définir cette notion. A notre sens, il semblerait même opportun de créer une catégorie juridique des données de connexion : ceci permettrait d'inclure ou exclure facilement les données, tout en adoptant une appellation commune. Cette délimitation sera indispensable à la détermination des régimes juridiques applicables à elle.

La difficulté de donner une définition des éléments contenus dans la notion de donnée de connexion nous amènera à étudier celle-ci dans un premier temps (section 1), en examinant les types d'informations qui peuvent être envoyés par l'internaute lorsqu'il est connecté, puis nous verrons dans quelle mesure ces données de connexion appréhendent les diverses législations (section 2). Cette approche aura le mérite de nous donner une vision de la donnée de connexion sous deux angles : l'angle technique et l'angle juridique.

Section 1. Les données de connexion, un moyen d'identification soumis à des exigences techniques

9. Concernant la détermination des éléments contenus dans une donnée de connexion, il est, à l'heure actuelle, très hasardeux de proposer une réponse précise et tranchée : la donnée de connexion est-elle un *log* de connexion, un témoin de connexion, ou encore toute donnée qu'un internaute peut émettre lorsqu'il est connecté sur Internet ?

Nous tenterons de donner la définition la plus précise et la plus claire possible, et pour cela, nous devrons envisager toutes les informations qu'un internaute transmet et reçoit lorsqu'il est connecté au réseau Internet et le cas échéant les inclure ou les exclure de la notion de donnée de connexion. Pour se faire, nous classerons les différentes données selon qu'elles relèvent de la catégorie des données de connexion sans soulever la moindre contestation (§1), selon qu'elles soulèvent discussion (§2).

Nous pouvons d'ores et déjà annoncer que la donnée de connexion doit être la donnée qui permet d'attester de la connexion d'un utilisateur au service. Nous nous baserons sur ce postulat afin d'étudier les différentes données.

§1. Les données relevant indiscutablement de la catégorie des données de connexion

10. L'association des fournisseurs d'accès désigne quelles informations sont collectées et conservées lors de la connexion de l'internaute au réseau[14]. L'association fait une distinction selon la personne qui récupère ces informations. Elle distingue ainsi entre les données de connexion à Internet collectées par le fournisseur d'accès[15] à Internet, les données de connexion

[14] Voir le site de l'association des fournisseurs d'accès <http://www.afa-france.com>

[15] Fournisseur d'accès : Définition publiée par la Commission de l'informatique et des composants électroniques le 13 mars 1999 : Organisme offrant à des clients d'accéder à l'Internet, ou, plus généralement, à tout réseau de communication. Le fournisseur d'accès peut aussi offrir des services en ligne.

Équivalent étranger : access provider

aux caches[16] collectées par l'opérateur de serveur cache et enfin les données de mise à jour du contenu hébergé relevées par l'hébergeur. S'il semble que les données de connexion à Internet et aux serveurs caches relèvent assurément des données de connexion, il apparaît néanmoins que les données de mise à jour du contenu hébergé n'en fassent pas incontestablement partie. C'est pourquoi nous étudierons ces informations dans le cadre des données soulevant discussion.

Nous suivrons ici la distinction faite par l'association des fournisseurs d'accès en étudiant dans un premier temps les données de connexion à Internet, puis ensuite les données de connexion aux serveurs caches.

A. Les données de connexion à Internet

11. Les données de connexion collectées et relevées par les fournisseurs d'accès à Internet comprennent divers éléments. Selon l'association des fournisseurs d'accès, ces éléments sont le *login* de l'utilisateur, l'adresse IP qui lui est affectée, et les dates et heures exactes de connexion et de déconnexion.

Si les dates et heures exactes de connexion et de déconnexion ne posent aucun problème, il en va autrement du *login* et de l'adresse IP.

Le *login* peut se présenter de différentes manières : ce peut être le nom de la personne abonnée au service, son adresse de courrier électronique[17], ou encore une suite illogique de signes. Lorsqu'il s'agit du nom de l'abonné, plusieurs cas de figure peuvent se poser : soit le seul nom, soit le nom

---

[16] Cache : Définition publiée par l'arrêté du 10 mars 1987 : Mémoire très rapide destinée à accélérer l'accès aux données les plus fréquemment utilisées. Cette mémoire est placée devant une autre mémoire moins rapide.

Synonyme : antémémoire, mémoire d'accès rapide

Équivalent étranger : cache memory, cache storage

[17] Courrier électronique : Définition publiée par la Commission de l'informatique et des composants électroniques le 20 juin 2003 : Libellé permettant l'identification d'un utilisateur de messagerie électronique et l'acheminement des messages qui lui sont destinés. L'adresse électronique est, dans le cas de l'Internet, constituée des identifiants de l'utilisateur et du gestionnaire de la messagerie, séparés par le caractère arrobe @. L'identifiant du gestionnaire de la messagerie comprend des désignations éventuelles de sous-domaines, celle d'un domaine, enfin un suffixe correspondant le plus souvent au pays ou au type d'organisme (exemples : .fr, .com).

Équivalent étranger : e-mail address

Forme abrégée : adresse électronique

et prénom, soit une contraction ou une combinaison de ceux-ci. Pour exemple, le *login* de M. Michel Dupont pourrait être : dupont, micheldupont, ou encore mdupont… Il est à noter que l'abonné au service se voit remettre un mot de passe corrélativement à son *login*. La pratique diffère selon les acteurs, mais le principe reste le même : le login est un moyen d'identification précis de l'abonné car il est unique. Deux abonnés ne peuvent avoir le même *login*.

L'adresse IP est nécessaire pour la reconnaissance des ordinateurs connectés au réseau. IP signifie Internet Protocol et désigne le protocole de communication en place sur le réseau, qu'il soit Internet ou intranet. Dans le cadre d'Internet, ce protocole est couplé avec le protocole TCP. L'adresse IP se présente sous la forme d'une suite de quatre nombres : 198.162.14.1 par exemple. Certaines adresses IP sont fixes, comme celles des serveurs par exemple, mais le cas est assez rare en pratique concernant les internautes. A chaque connexion de l'internaute sur le réseau, le fournisseur d'accès à Internet attribuera à son ordinateur une adresse IP valable pour le temps de sa session.

La donnée de connexion collectée et conservée par le fournisseur d'accès à Internet constitue donc la donnée de connexion par excellence de par sa fonction : c'est la donnée collectée par le fournisseur d'accès chaque fois que l'internaute se connecte au réseau Internet.

B. Les données de connexion aux caches

12. La mémoire cache a pour objet d'accélérer la communication et la consultation des informations sur le réseau. En réalité, il faut distinguer les caches utilisés par les fournisseurs d'accès par le biais d'un serveur de cache (*proxy*[18]) et ceux stockés sur le disque dur de notre ordinateur. Nous écarterons ici les données caches contenus sur la machine de l'internaute pour nous focaliser sur celles contenues par les serveurs des fournisseurs d'accès (serveurs *proxy*).

L'association des fournisseurs d'accès donne sur son site web la liste des éléments contenus par les données de connexion collectées et conservées par les opérateurs de serveurs caches. Ces données de connexion comprennent donc l'adresse IP de l'internaute, le nom du serveur requis

[18] Proxy : Définition publiée par la Commission de l'informatique et des composants électroniques le 16 mars 1999 : Dispositif informatique associé à un serveur et réalisant, pour des applications autorisées, des fonctions de médiation, telle que le stockage des documents les plus fréquemment demandés ou l'établissement de passerelles.
Équivalent étranger : Serveur mandataire, passerelle

par l'utilisateur (c'est-à-dire le site Internet[19]), le document demandé et les dates et heures exactes.

Nous pouvons constater que ce type de donnée de connexion nécessite plus d'informations que les simples données de connexion à Internet précédemment exposées. En effet, outre l'IP et les dates et heures exactes, sont ici collectées des informations relatives au nom du serveur et au document demandé.

Bien que la donnée de connexion aux serveurs caches n'ait pas le même caractère que celui de la donnée de connexion à Internet, il n'en demeure pas moins qu'elle fait partie de la catégorie des données de connexion. Il ne faut en effet pas tenir compte du fait que cette technique soit indispensable à la connexion et à la navigation sur le réseau. L'internaute, pour se connecter à Internet, devra passer par les serveurs de cache. De plus, nous pouvons arguer que la donnée de connexion aux serveurs caches contient l'élément principal d'identification de l'internaute : son adresse IP couplée aux dates et heures exactes de connexion et de déconnexion.

§2. Les données soulevant discussion quant à leur intégration dans la catégorie des données de connexion

13. Ce sont principalement les données n'étant pas considérés par les prestataires techniques comme des données de connexion *stricto sensu*. Toutefois ces données peuvent témoigner de la connexion d'un internaute au réseau : en ce sens elles doivent être considérées comme des données de connexion.

A. Les données de mise à jour du contenu des hébergeurs

14. Selon l'association des fournisseurs d'accès à Internet, les données de connexion englobent aussi les données de mise à jour du contenu hébergé. Ces données sont collectées et conservées

[19] Site Internet : Définition publiée par la Commission de l'informatique et des composants électroniques le 8 décembre 2002 : Ensemble de documents et d'applications placés sous une même autorité et accessibles par la toile à partir d'une même adresse universelle. Un site de la toile peut être inclus dans un site plus important.
Équivalent étranger : web site

par le fournisseur d'hébergement et contiennent le *login* de l'utilisateur, l'adresse IP qui lui est affectée par son fournisseur d'accès et les dates et heures exactes de connexion et de déconnexion. Nous pouvons constater que les données collectées sont quasiment les mêmes que celles collectées par le fournisseur d'accès à Internet.

En réalité si ce type d'information se trouve au milieu des données de connexion sur le site de l'AFA, la raison en est que, très souvent, les fournisseurs d'accès à Internet sont également des fournisseurs d'hébergement, c'est-à-dire qu'ils mettent à la disposition de leurs abonnés un espace sur leurs serveurs afin que ceux-ci puissent élaborer des pages personnelles. En faisant cela ils ont donc une double fonction : assurer la connexion au service et fournir un espace disque sur leurs serveurs. Pour autant, pouvons-nous encore parler de données de connexion ? En effet, tous les internautes n'utilisent pas cette fonction, et tous les fournisseurs d'accès n'assurent pas une telle offre. Il ne nous semble pas qu'il soit nécessaire de distinguer selon que l'internaute ait accès ou utilise l'hébergement offert par son fournisseur d'accès : si l'internaute ne dispose pas de ce service alors de telles données ne seront pas collectées, en revanche si il l'utilise elles le seront. Pour l'internaute bénéficiant d'un hébergement chez son fournisseur d'accès à Internet, ce seront de véritables données de connexion qui seront collectées au même titre que les données collectées par l'opérateur dans sa fonction de fourniture d'accès. Nous pouvons noter que la combinaison est similaire : *login*, adresse IP et dates et heures de connexion et déconnexion.

Cette conception se veut être la plus large possible, il ne semble pas opportun de laisser de côté certaines informations du fait qu'elles ne concernent qu'une certaine catégorie d'internautes. Car le fait de mettre à la disposition d'autres internautes du contenu informationnel par le biais de son fournisseur d'accès et d'hébergement n'enlève nullement la qualité d'internaute.

B. Les cookies

15. Un cookie est un code qu'un serveur http enregistre, souvent temporairement, sur le disque dur de l'internaute pour l'identifier sur son service. Selon la définition de la C.N.I.L., le cookie est enregistré sous la forme d'un fichier texte sur le disque dur de l'ordinateur client, qui comprend des informations que le serveur pourra aller relire et modifier par la suite. Etant donné que le cookie repose sur le protocole http, on ne peut trouver de cookie que sur le web (qui n'est, rappelons le, qu'une partie du réseau Internet). Les champs qui composent le cookie sont donc

stockés dans le fichier texte enregistré sur l'ordinateur client, c'est-à-dire celui de l'internaute. Il est à noter que l'accès au cookie n'est offert qu'à la personne possédant le nom de domaine qui y est attaché, c'est-à-dire le webmestre[20].

A l'évidence, le cookie n'est pas une donnée essentielle à la connexion de l'internaute au réseau Internet, d'une part car de nombreux sites n'utilisent pas cette technique et car le cookie ne concerne que le web, et d'autre part car le cookie n'assure pas la même fonction de fourniture de connexion au réseau à l'internaute, comme peut le faire la donnée de connexion collectée par le fournisseur d'accès. Cependant force est de constater qu'aujourd'hui le cookie a pris une place prépondérante sur le paysage de l'Internet mondial : aussi de nombreux sites http n'assurent pas l'accès aux internautes ayant refusé de recevoir des cookies. De plus, lorsqu'il a accepté de recevoir des cookies, l'internaute laisse derrière lui de nombreuses traces des connexions aux sites qu'il a visité. En ce sens, nous pouvons considérer que si le cookie n'est pas une donnée permettant la connexion à Internet, il n'en demeure pas moins qu'il atteste de la connexion de l'internaute. En attestant de cette connexion, le cookie pourra permettre l'identification de l'internaute. En ce sens, il nous apparaît qu'il doit être appréhendé par le droit comme une donnée de connexion de l'internaute.

C. L'IP et l'IPv6

16. L'IP est, comme nous l'avons dit, indispensable sur Internet dans l'identification des machines connectées. L'IP est « une adresse codée sur 32 bits selon le protocole Internet et affectée à un ordinateur figurant sur le réseau. Une portion de l'adresse IP désigne le réseau et l'autre désigne un ordinateur dans ce réseau »[21]. Cependant, il nous semble que pour que l'adresse IP soit considérée comme une donnée de connexion, il lui est nécessaire d'être combinée à d'autres éléments. Ceci se retrouve dans le cadre des données de connexion collectées par le fournisseur d'accès à Internet par exemple, où elle est associée au login de l'utilisateur et aux heures exactes de connexion et de déconnexion. Toutefois, ne pourrions-nous

[20] Webmestre : Définition publiée par la Commission de l'informatique et des composants électroniques : Personne chargée de la maintenance et du suivi d'un site ou d'un serveur sur la toile d'araignée mondiale.

Équivalent étranger : webmaster

[21] Groupe SOS Informatique, glossaire informatique <www..sos-informatique.gc.ca>

pas considérer que l'adresse IP couplée aux seules dates et heures de connexion et de déconnexion puisse être considérée comme une donnée de connexion ? L'adresse IP attesterait alors de la connexion de l'internaute au réseau à tel moment. Par là, cette information pourrait être envisagée comme une véritable donnée de connexion de l'internaute.

La solution sera renforcée lorsque l'internaute disposera de la part de son fournisseur d'accès à Internet d'une adresse IP fixe, c'est-à-dire qui ne changerait pas à chaque cycle de connexion. Dans cette optique, l'adresse IP fixe attestera sans aucune contestation possible de la connexion de l'internaute au réseau à chaque fois que cette adresse IP sera « disponible ».

L'IPv6 est une version avancée de l'actuel IP, et devrait le remplacer d'ici une vingtaine d'années. Ce remplacement est dû au fait de la saturation du nombre d'adresses IP pouvant être affectées actuellement. L'IPv6 peut être rapprochée de la notion d'adresse IP fixe, puisqu'il semble acquis que ce nouveau type d'adresse sera unique pour chaque ordinateur connecté : l'adresse contiendra une partie qui identifiera à coup sûr la machine. Cette adresse sera, comme l'IP, envoyée et collectée par les différents acteurs chaque fois que l'internaute se connectera sur Internet. En ce sens, l'adresse IP pourra apparaître comme une donnée de connexion, sans qu'il ne soit impérativement nécessaire de la coupler avec d'autres informations.

D. Les variables de connexion

17. Les variables d'environnement permettent de faciliter le travail des programmes en plaçant des informations disponibles par d'autres applications. Ces variables d'environnement sont essentiellement contenues dans le navigateur. Lors de la navigation sur Internet, ces variables permettront au serveur web de prendre connaissance de ces informations telles que la version du navigateur, du système d'exploitation[22] ou encore de la dernière page web visitée.

Ces variables vont donc offrir au serveur la connaissance des connexions effectuées par l'internaute sur les sites précédemment consultés. Or il ne s'agit pas ici de données de connexion à proprement parler étant donné que l'internaute mais nous pouvons considérer qu'en diffusant

[22] Système d'exploitation : Définition publiée par l'arrêté du 22 décembre 1981 : Logiciel gérant un ordinateur, indépendant des programmes d'application mais indispensable à leur mise en oeuvre
Équivalent étranger : operating system

des informations sur des éléments pouvant se rapporter à l'internaute en combinaison d'une adresse IP par exemple, ces variables de connexion puisse être considérées comme des données de connexion.

E. Les données ne relevant pas de la catégorie des données de connexion

18. La mémoire cache se trouvant sur la machine de l'internaute est l'une des formes de données de cache (l'autre étant celle se trouvant sur un serveur *proxy*). Ici le navigateur laissera une trace des pages consultées sur la machine de l'internaute et non pas sur un serveur distant. Cette mémoire « locale » n'interagit pas avec celle contenue sur le serveur du fournisseur d'accès, mais peut être considérée comme une donnée de connexion : en effet, si un tiers consulte cette mémoire après l'utilisation d'Internet par une autre personne, il pourra savoir ce que ce dernier aura consulté… Nous pouvons donc dire que c'est une donnée de connexion.

19. Au regard des éléments développés, plusieurs types de données entrent dans la catégorie des données de connexion. Telle que nous la définissions, la donnée de connexion est la donnée qui atteste de la connexion d'un internaute au réseau. Cette définition permet d'englober les données permettant la connexion de l'internaute à Internet telles que les données de connexion collectées par le fournisseur d'accès et les données de connexion aux serveurs caches, ainsi que les données attestant de la connexion d'un utilisateur à Internet telles que les témoins de connexion[23] que sont les cookies. Il apparaît donc un critère de l'appartenance à la catégorie des données de connexion qui est l'attestation de la connexion de l'internaute au service.

[23] Témoin de connexion : Définition publiée par la Commission de l'informatique et des composants électroniques le 16 mars 1999 : Appliquette envoyée par un serveur de la toile mondiale à un utilisateur, parfois à l'insu de celui-ci, au cours d'une connexion afin de caractériser cet utilisateur. Par extension, information que l'appliquette peut enregistrer sur le disque de l'utilisateur et à laquelle le serveur peut accéder ultérieurement. Dans cette acception, on dit aussi « mouchard ».

La catégorie des données de connexion n'est donc pas une catégorie homogène : s'y retrouvent des données de connexion à proprement parler mais aussi d'autres types de données tels que les témoins de connexion. Cette catégorie a aussi comme caractéristique de ne pas être figées et sera amenée à s'adapter aux progrès de la technique et à l'apparition de nouvelles données de connexion. Les données de connexion en devenir devront répondre au critère de certification de la connexion de l'internaute.

Après avoir posé le critère d'une donnée de connexion, il convient de déterminer quels régimes juridiques peuvent s'appliquer à elle.

Section 2. Les données de connexion, un moyen d'identification soumis à des exigences juridiques

20. De plus en plus de personnes se connectent quotidiennement au réseau Internet. Leurs activités peuvent être nombreuses : *chat*, participation à des forii[24] de discussion, simple navigation, envoi de courriers électroniques[25]… Souvent ces personnes ne se doutent pas des atteintes dont elles sont susceptibles d'être la cible. Plus exactement, ce sont les données de connexion que ces personnes divulguent sur Internet qui suscitent la convoitise. Afin de garantir la protection de ces précieuses informations, il est nécessaire de déterminer le régime juridique applicable à celles-ci. Dans ce dessein, il faut confronter les données de connexion de l'internaute aux régimes de protection des droits de la personne, notamment la protection de la vie privée, qui comprend la protection du secret des correspondances, et enfin la protection des données à caractère personnel et des informations nominatives.

§1. Données de connexion et droit des données à caractère personnel

21. Le droit des données à caractère personnel est régi en France par des dispositions nationales mais aussi par des dispositions d'ordre communautaire.

---

[24] Forum : Définition publiée par la Commission de l'informatique et des composants électroniques : Service permettant discussions et échanges sur un thème donné : chaque utilisateur peut lire à tout moment les interventions de tous les autres et apporter sa propre contribution sous forme d'articles. Par extension, on désigne également par ce terme les systèmes de discussion télématiques, qui offrent généralement un service de téléchargement (connus en anglais sous le nom de BBS, *Bulletin Board System*).

Équivalent étranger : newsgroup

[25] Courrier électronique : Définition publiée par la Commission de l'informatique et des composants électroniques : Document informatisé qu'un utilisateur saisit, envoie ou consulte en différé par l'intermédiaire d'un réseau. Un courriel contient le plus souvent un texte auquel peuvent être joints d'autres textes, des images ou des sons. Par extension, le terme «courriel» et son synonyme « courrier électronique » sont employés au sens de « messagerie électronique ».

Synonyme : message électronique

Équivalent étranger : e-mail, electronic mail

En France, la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés régit le droit des données à caractère personnel. Elle constitue le pilier central de la législation française sur la protection des informations nominatives. Nous pouvons noter que la loi n'envisage pas les données à caractère personnel mais les informations nominatives. Toutefois il semble admis que l'on puisse considérer ces notions comme équivalentes.

Il conviendra donc de déterminer dans quelle mesure les données de connexion de l'internaute peuvent être considérées comme des données à caractère personnel. Au niveau européen, la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 constitue la législation de base de la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

Selon l'article 4 de la loi de 1978, « *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* ».

L'article 2 de la directive définit les données à caractère personnel comme étant « *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* ».

De ces deux articles, il ressort que les données à caractère personnel doivent posséder certaines caractéristiques : ce sont des informations qui permettent, de manière directe ou indirecte, d'identifier une personne physique. La directive semble néanmoins plus précise car elle envisage le cas de la personne identifiable, qui n'est qu'une possibilité d'identification.

Il convient d'ajouter une autre condition d'application des textes relative à la protection des données à caractère personnel : ces données doivent faire l'objet d'un traitement. Le traitement est défini par le directive de 1995 comme « *toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliqués à des données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le*

verrouillage, l'effacement ou la destruction ». La directive définit également la notion de responsable du traitement dans son article 2d comme « *la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel ; lorsque les finalités et les moyens du traitement sont déterminés par des dispositions législatives ou réglementaires nationales ou communautaires, le responsable du traitement ou les critères spécifiques pour le désigner peuvent être fixés par le droit national ou communautaire* ». Ces définitions du traitement et du responsable du traitement sont reprises par le projet de loi de transposition de la directive. Il s'avèrera assez simple de prouver que dans notre domaine, les données aient fait l'objet d'un traitement, puisque celui-ci n'exige pour exister qu'un simple enregistrement de la donnée. Dans tous les cas, que la donnée soit un cookie, l'adresse IP, ou encore une donnée de connexion, il y aura constamment un traitement de celle-ci. Il reste alors à prouver le caractère personnel des données. Pour cela, nous distinguerons entre les origines des données, selon qu'elles aient été collectées par le fournisseur d'accès et par l'hébergeur, ou selon qu'elles aient été collectées par d'autres personnes.

A. Les données collectées par les fournisseurs d'accès et d'hébergement

22. Ces données sont les données de connexion à Internet, les données de connexion aux serveurs caches et enfin les données de mise à jour du contenu hébergé. Ces données sont des données de connexion mais peuvent-elles pour autant être vues comme des données à caractère personnel ?

Les données de connexion à Internet sont comme nous l'avons vu constituées par le *login* de l'utilisateur, l'adresse IP qui lui est affecté ainsi que les dates et heures de connexion et de déconnexion. Les données de connexion aux serveurs caches comportent l'adresse IP affectée à l'utilisateur ainsi que les dates et heures de connexion et de déconnexion. Enfin les données de mise à jour du contenu hébergé collectées par l'hébergeur comprennent le *login* de l'utilisateur, son adresse IP et enfin les dates et heures de connexion et de déconnexion.

Le *login* est donc un nom d'utilisateur qui permet à ce dernier de s'identifier auprès du fournisseur de service afin qu'il puisse justifier de son identité. Le login est parfois anonymisé mais rien n'empêche qu'il puisse être le nom patronymique de l'utilisateur, ou encore son adresse de courriel. Lorsqu'il n'est pas anonymisé, le login est clairement et incontestablement une

donnée qui permet d'identifier directement une personne physique et l'application de la législation sur les données à caractère personnel s'applique pleinement. Lorsque le *login* est une suite illogique de signes, ou encore un pseudonyme, il n'en demeure pas moins qu'il fait référence, dans la base de données du fournisseur de service, à la véritable identité de la personne utilisatrice de ce service. Cette base de données constituerait en outre un traitement au sens de la législation relative à la protection des données à caractère personnel. Cette condition de la réalisation d'un traitement est nécessaire à l'application de cette législation, et en pratique, on peut penser qu'elle sera toujours remplie en ce qui concerne les données collectées par les fournisseurs d'accès et d'hébergement. En tout état de cause, nous serions ici en présence d'une donnée qui permet d'identifier indirectement la personne qui se trouve derrière ce login. Il serait plus que facile pour le fournisseur d'accès ou d'hébergement de faire l'association entre une personne et son login. Là encore l'application des règles régissant la protection des données à caractère personnel se trouverait mise en œuvre.

L'adresse IP est une donnée très importante car elle permet d'identifier très facilement la machine connectée au réseau, et donc par là même, l'abonné qui l'utilise. L'adresse IP semble faire partie du champ d'application de la directive de 1995. Dans son article 2, la directive dispose que « *est réputée identifiable une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification* ». L'adresse IP est sans aucun doute un numéro d'identification de l'abonné sur le réseau. En complément, le considérant 26 de la directive dit que « *pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens susceptibles d'être raisonnablement mis en œuvre, soit par le responsable du traitement, soit par une autre personne, pour identifier ladite personne* ». L'identification de l'abonné au service pourra se faire sans aucun problème par le fournisseur en regroupant l'adresse IP qui avait été affectée à l'utilisateur avec les dates et heures exactes de connexion et de déconnexion. Nous pouvons considérer que l'adresse IP est une donnée qui permet l'identification de la personne abonnée au service, et ce de manière indirecte. L'adresse IP est donc une donnée indirectement à caractère personnel. Toutefois il est aussi acquis que l'adresse IP en elle-même n'est pas une donnée à caractère personnel et qu'elle nécessite d'être couplée avec les dates et heures exactes de connexion et déconnexion afin de tomber sous le joug du droit des données à caractère personnel. En effet, l'adresse IP changeant à chaque connexion, elle ne peut permettre seule à rendre une personne identifiable. Les dates et heures de connexion

exactes recueillies chez le fournisseur d'accès devront être recoupées avec l'adresse IP pour déterminer le login qui l'a utilisé pendant cette période.

En ce qui concerne les données de connexion aux serveurs caches, celles-ci semblent être exclues du champ d'application de la loi de transposition de la directive de 1995. En effet l'article 4 du projet de loi dispose que ces dispositions « *ne sont pas applicables aux copies temporaires qui sont faites dans le cadre des activités techniques de transmission et de fourniture d'accès à un réseau numérique, en vue du stockage automatique, intermédiaire et transitoire des données et à seule fin de permettre à d'autres destinataires du service le meilleur accès possible aux informations transmises* ». Ceci signifierait purement et simplement que les données de connexion aux serveurs caches ne seraient pas considérées comme des données à caractère personnel de l'internaute. Toutefois, l'IP contenu dans ces données pourra lui-même être considéré comme une donnée à caractère personnel. Un doute subsiste donc sur la qualification des données de connexion aux serveurs proxy…

En ce qui concerne l'IP fixe et plus tard l'IPv6, l'identification se fera beaucoup plus simplement étant donné que chaque machine disposera d'une adresse unique. A cet égard, le groupe de travail de l'article 29 estime, dans l'avis 2/2002 relatif à l'utilisation d'identifiants uniques dans les terminaux de télécommunications (exemple de l'IPv6) en date du 30 mai 2002, que « *les adresses IP attribuées aux internautes sont des données à caractère personnel et sont protégées par les directives UE 95/46 et 97/66* ».

Les conditions d'identification et de traitement étant remplies, nous pouvons donc affirmer, en ce qui concerne les données relevées par les fournisseurs d'accès et d'hébergement, que ces données de connexion sont clairement des données à caractère personnel justifiant l'application de la loi de 1978 et de la directive de 1995.

B. Le cas des cookies

23. Les cookies peuvent être considérés comme des données de connexion, comme nous l'avons évoqué précédemment. Pour autant les cookies peuvent-ils être considérés comme des données à caractère personnel ? La directive 95/46/CE du 24 octobre 1995 précitée définit la donnée à caractère personnel comme étant celle qui identifie ou rend identifiable, directement ou indirectement, une personne physique. Or un cookie permet-il cette identification ?

Dans le cas des cookies de session, il semble acquis que celui-ci ne puisse être considéré comme une information nominative car son but est essentiellement technique et sont détruits automatiquement lorsque l'utilisateur ferme la session ouverte sur le site Internet.

En revanche, différent est le cas des cookies rémanents car ceux-ci permettent au serveur d'accéder aux informations qu'ils contiennent à chaque connexion audit serveur. C'est ce type de cookie qui nous intéressera donc ici.

A priori, un cookie n'est pas nominatif à lui seul. Le cookie a comme principal avantage de ne pas encombrer les serveurs des hôtes, en étant stocké sur l'ordinateur client. A l'origine le cookie n'avait pas pour vocation à identifier les visiteurs d'un site Internet. Aujourd'hui la situation a changé et le cookie sert souvent à identifier l'internaute. Ceci est clair lorsque l'internaute remplit un formulaire sur un site web qui fonctionne avec des cookies. Il sera alors envisageable que ce site enregistre les informations entrées par l'internaute sur ce ou ces cookies. Dans le cas où l'internaute entre ces coordonnées personnelles sur le site, et que ce dernier les enregistre dans un fichier sur la machine de l'internaute, alors le cookie peut assurément devenir une donnée à caractère personnel au sens de la directive de 1995. Le serveur pourra identifier de manière très certaine l'internaute chaque fois que celui-ci s'y connectera. En outre, même dans le cas où l'internaute ne remplit pas un formulaire, le cookie contient très souvent dans son texte l'identité que l'utilisateur de l'ordinateur aura donné lors de l'enregistrement de la copie de son système d'exploitation. Le cookie est alors une donnée à caractère personnel telle qu'envisagée par la législation sur la protection des personnes à l'égard des traitements automatisés de données à caractère personnel. La condition du traitement sera elle aussi remplie car le site Internet fera une utilisation de ces informations, qui est une des formes de traitement.

De plus, la directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques fait référence à la directive protection des données à caractère personnel de 1995 à propos des cookies dans son considérant 25. « *Leur utilisation* (des cookies) *devrait être autorisée à condition que les utilisateurs se voient donner des informations claires et précises, conformément à la directive 95/46/CE, sur la finalité des témoins de connexion ou des dispositifs analogues de manière à être au courant des informations placées*

sur l'équipement terminal qu'ils utilisent ». Cette référence semble inclure de manière certaine le cookie dans le champ d'application de la directive mère de 1995.

§2. Données de connexion et droit à la vie privée

24. Les données de connexion peuvent-elles mettre en péril la vie privée des internautes ? Afin de répondre à cette question, nous envisagerons le cas des données de connexion dans le cadre de la vie privée en elle-même puis dans le cadre particulier des correspondances.

A. Le droit à la vie privée proprement dit

25. L'article 9 du code civil pose un principe fondamental dans la protection des personnes en disposant que « *chacun a droit au respect de sa vie privée* ». Ce principe s'applique évidemment dans le domaine de l'informatique et de l'Internet. Cette exigence se trouve aujourd'hui dans la directive 97/66/CE du Parlement européen et du Conseil du 15 décembre 1997 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications et dans la directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques.

L'article 1 de la directive de 2002 dispose que « *la présente directive harmonise les dispositions des Etats membres nécessaires pour assurer un niveau équivalent de protection des droits et libertés fondamentaux, et en particulier du droit à la vie privée, en ce qui concerne le traitement des données à caractère personnel dans le secteur des communications électroniques* ». Il convient donc d'étudier la soumission de données de connexion de l'internaute au droit à la vie privée à la lumière de cette directive. Cette directive pose des principes concernant la conservation des données relatives au trafic, notamment en ce qui concerne la durée de conservation et le type d'informations conservées. Or les données relatives au trafic sont définies par l'article 2 comme étant « *toutes les données traitées en vue de l'acheminement d'une communication par un réseau de communications électroniques ou de sa facturation* ». Nous pouvons constater que cette définition peut recouper celle des données de connexion collectées par les fournisseurs d'accès à Internet, par les opérateurs de serveurs caches et par les

fournisseurs d'hébergement. En effet, ces données de connexion sont des données transmises par l'utilisateur lorsque celui-ci se connecte au service et ont pour objectif la réalisation et l'optimisation de la connexion ainsi que la facturation. Ces données se voient donc appliquer les dispositions de la directive vie privée et communication électronique du 12 juillet 2002.

En ce qui concerne les cookies, ceux-ci sont aussi visés par la directive 2002/58/CE, dans son considérant 25. Ceci est logique dans la mesure où les cookies peuvent réellement porter atteinte au droit à la vie privée dont dispose l'internaute, notamment en ce qui concerne les cookies rémanents. Nul doute qu'une atteinte à la vie privée par l'intermédiaire de cookie serait sanctionnée.

Une atteinte à la vie privée de l'internaute pourra être aisément envisageable par la biais de ces données de connexion lorsque celui-ci est tracé sur le réseau, et que l'on accède aux sites qu'il visite le plus régulièrement. Ce type d'atteinte doit évidemment être sanctionné.

B. La législation sur les correspondances

26. La loi n° 91-646 du 10 juillet 1991 est le texte de référence concernant le secret des correspondances émises par la voie des télécommunications. Ce dispositif de protection peut être considéré comme faisant partie du domaine de la protection de la vie privée. Il protège les correspondances dites privées qui impliquent qu'il doit exister une relation personnelle entre l'émetteur et le récepteur, mais aussi une relation personnelle entre l'objet du message et les personnes concernées.

La directive 2002/58/CE du 12 juillet 2002 concerne la protection de la vie privée dans le secteur des communications électroniques. Nous pourrions en déduire par là qu'elle concerne aussi les correspondances échangées par voie électronique qu'elle définit comme tout message envoyé par un réseau public de communications. Il semble donc que la législation sur les correspondances privées puisse s'appliquer pour les données de connexion relatives à la communication de ce type de correspondance.

Les données de connexion sont, comme nous l'avons démontré, des données attestant de la connexion d'un internaute au réseau Internet. De par leur qualité et leur contenu, ces données permettent à l'internaute de bénéficier d'une certaine protection de celles-ci.

Une difficulté se pose néanmoins quant à la détermination du sujet de la protection tant l'internaute semble difficile à délimiter.

Chapitre 2. L'internaute : entre identification et personnalisation

27. A l'heure actuelle, aucune mention à l'internaute n'est faite dans les textes normatifs et les auteurs n'ont pas apporté de qualification pour cet individu. L'internaute est donc appréhendé comme une personne virtuelle évoluant dans un monde tout aussi virtuel. Pourtant, il peut arriver que dans certaines situations, il y ait un besoin de matérialiser l'internaute.

Il devient alors nécessaire de déterminer l'internaute et se poseront ici les plus grandes difficultés. L'internaute est défini communément comme l'utilisateur de l'Internet. Cette définition qui n'a rien de juridique doit-elle être conservée ? (section 1)

La détermination de la personne de l'internaute s'avèrera donc nécessaire afin de lui faire bénéficier de la protection et des garanties offertes par les diverses législations protectrices des personnes (section 2).

Section 1. L'internaute, une personne difficilement déterminable

28. Cette difficulté de détermination de l'internaute pose la question de savoir qui est finalement l'internaute. A première vue, il devrait s'agir de celui qui utilise l'Internet. Mais, cette perspective peut poser de nombreuses complications tant il pourra être difficile de prouver qui utilisait effectivement l'ordinateur à un instant précis. C'est pourquoi l'on pourrait être tenté de dire que l'internaute est la personne abonnée au service Internet chez un fournisseur d'accès. Ici encore, la réponse n'est pas satisfaisante…

Nous étudierons donc chacune des deux conceptions afin de déterminer laquelle peut légitimement avoir sa place en tant qu'instrument d'application des droits de la personne : en premier lieu l'internaute comme étant l'abonné au service et dans un second temps l'internaute comme tout utilisateur d'Internet.

§1. Une conception restreinte de l'internaute : l'internaute comme abonné au service

29. Envisager l'internaute comme abonné du service permet une grande simplicité d'identification puisqu'il suffit de se renseigner chez le fournisseur d'accès pour connaître l'identité de celui-ci. De plus les données de connexion telles que nous les avons étudiées font pour la plupart une référence expresse à l'abonné (la donnée de connexion collectée par le fournisseur d'accès à Internet et par l'opérateur de serveurs caches). Cela ne signifie par pour autant que l'identification d'un utilisateur d'Internet autre que l'abonné sera impossible à réaliser. Ainsi, malgré ces arguments, il faut soulever le fait que cette théorie n'est pas représentative de l'utilisation de l'Internet et de nos habitudes. C'est pourquoi nous pensons qu'*a priori* une conception large doit être acceptée. Afin de juger de la qualité et de la pertinence d'une telle affirmation, nous suivrons une démarche qui consistera à étudier quels sont les avantages et les inconvénients de ce système.

A. Intérêts de la conception de l'internaute-abonné

30. Les données de connexion ne permettent pas toujours d'accéder à la personne qui utilise la machine. Lorsqu'il s'agira des données de connexion relatives à l'accès Internet, à l'accès aux serveurs de mémoire cache ou encore à l'hébergement d'un contenu, la donnée de connexion permettra d'identifier l'abonné au service fourni par le fournisseur d'accès à Internet ou par le fournisseur d'hébergement. Lorsqu'il s'agira de l'adresse IP, cette donnée de connexion renverra à la machine et non pas à la personne derrière la machine.

L'intérêt de considérer comme internaute la seule personne bénéficiant d'un abonnement chez un fournisseur de service permet une authentification rapide et simplifiée des personnes navigant sur la toile mondiale.

B. Inconvénients de la conception de l'internaute-abonné

31. L'inconvénient majeur de cette conception est de ne pas offrir une vision conforme à la réalité : en ne considérant l'internaute comme ne pouvant être que l'abonné au service offert par le fournisseur d'accès à Internet, cette conception laisse certaines personnes hors du droit. En effet quel sort peut être réservé aux autres membres de la famille, aux clients d'un cybercafé, aux usagers d'une université ou encore aux salariés d'une entreprise ?

Malgré une identification aisée, il n'en demeure pas moins qu'il s'agit d'un travestissement de ce qu'il se passe concrètement. Pour ces raisons, nous nous tournerons vers une conception plus large de la personne de l'internaute, même si des obstacles, notamment au niveau de l'identification, se dressent.

§2. Une conception large de l'internaute : l'internaute comme utilisateur du service

32. Si définir l'internaute comme l'utilisateur de l'Internet se confond parfaitement à la réalité, il n'en demeure pas moins que ceci peut poser de nombreux soucis lorsqu'il s'agira de conférer des droits aux internautes ou de les poursuivre… Nous suivrons la même démarche que celle de l'étude de l'internaute-abonné, en étudiant tout d'abord les intérêts d'une telle hypothèse, puis en en voyant les désavantages.

A. Intérêts de la conception de l'internaute-utilisateur

33. L'intérêt principal de voir l'internaute comme étant un utilisateur est qu'il permet d'envisager l'exhaustivité des situations se présentant en pratique.

De plus, cette conception correspond à la définition de l'internaute telle qu'elle est donnée par le Lamy Droit des médias et de la communication dans son édition 2003 : l'internaute est la « *personne physique utilisant Internet et notamment les ressources disponibles sur le WWW*[26] ». Le Lamy Droit de l'informatique et des réseaux, dans son édition 2003 définit l'internaute comme l'utilisateur d'Internet. Ces définitions ne font nullement apparaître la notion d'abonné. Le cybernaute ne se définit donc pas comme l'abonné au service mais comme l'utilisateur du service.

Cette conception permet ainsi de prendre en compte un très grand nombre de situations. Ainsi une des utilisations les plus courantes de l'Internet se fait au domicile, dans les foyers. Comme nous l'avons vu, ne tenir compte que de l'abonné nous contraint à occulter le fait que d'autres personnes comme le conjoint, les enfants, ou même un colocataire, puissent utiliser Internet. En revanche, considérer chaque utilisateur de la prestation comme un internaute permet d'assurer à chacun d'entre eux des droits concernant leur vie privée. Ainsi, si l'un d'entre eux subit une atteinte concernant par exemple ses données personnelles, il pourra alors agir devant la C.N.I.L.. En outre, il arrive que dans les foyers, chacun puisse avoir sa propre session d'ouverture dans le système d'exploitation de l'ordinateur familial. Ici la situation est encore plus flagrante, car chaque membre du foyer agit à sa guise sur son propre espace dans l'ordinateur. Certains fournisseurs d'accès offrent aussi la possibilité à chaque membre de la famille de disposer de son propre login et de son propre mot de passe. Il devient alors très simple pour le fournisseur d'accès d'identifier parfaitement quelle personne utilise le service à un moment donné. Il sera très réducteur de ne considérer que l'abonné à Internet, alors que chacun peut être identifié directement !

[26] World wide web : expression littéralement traduite par « toile d'araignée mondiale » et désignant un service interactif proposé sur Internet par l'intermédiaire d'un logiciel client appelé navigateur.
Le World wide web permet d'accéder, grâce à un protocole normalisé de diffusion de l'information, le http, à des ressources considérables à travers des sites tous réalisés à partir d'un langage unique : le HTML. Définition du Lamy Droit des médias et de la communications, édition 2003.

D'autres domaines peuvent être concernés en dehors du cadre familial. Un des exemple les plus frappant est celui des cybercafés[27] et des établissements proposant des Hot Spots[28]. Le propriétaire du cybercafé ou de l'établissement proposant le Wi-fi sera en règle générale l'abonné au service. Pour autant devra-t-il être considéré comme l'internaute ? Une telle solution semblerait absurde tant il est évident que ce sont les clients ou les usagers qui doivent être considérés comme internautes, car ce sont eux les utilisateurs. Il pourrait se poser un problème d'identification de chaque personne ayant utilisé les machines mises à disposition, mais ce problème est contournable en pratique. Dans le cadre des établissements Hot Spot, il suffira d'attribuer des adresses IP aux clients en prenant soin de récupérer leurs coordonnées et les dates et heures exactes de connexion et de déconnexion, de la même manière que le font les fournisseurs d'accès. Ainsi la tenue d'un registre permettra d'identifier qui a utilisé la connexion à un moment précis. Le principe pourrait être le même dans un cybercafé.

Il existe un autre domaine dans lequel l'abonné n'est pas l'utilisateur du service : il s'agit du monde de l'entreprise. L'utilisation d'Internet dans le secteur du travail est devenu aujourd'hui quasi-indispensable. La société est la plupart du temps l'abonnée au service, mais ce sont les salariés qui utilisent le réseau à des fins professionnelles, ou à des fins personnelles selon la tolérance accordée. Là encore, il sera assez aisé de connaître l'identité d'une personne qui souhaite faire valoir ses droits : souvent les postes ont chacun une adresse IP fixe attribuée par l'administrateur réseau.

Bien entendu, ces illustrations n'ont pas une valeur absolue, elles visent à démontrer que, dans de nombreuses situations, il est inconcevable de réduire la qualité d'internaute au seul abonné au service.

B. Inconvénients de la conception de l'internaute-utilisateur

34. Le principal reproche que l'on peut faire à cette conception est qu'il peut apparaître comme difficile de désigner une personne qui n'est pas l'abonné. Nous l'avons vu, en pratique, ce

[27] Café ayant pour principe de proposer un accès Internet en l'échange d'un paiement.

[28] Le Hot Spot permet aux personnes possédant un ordinateur portable de pouvoir se connecter sur un réseau sans fil (dit Wi-fi). De nombreux établissements proposent ce service aujourd'hui, ainsi que des administrations telles que les facultés.

problème peut être évité. Cependant imaginons que dans un cybercafé, le propriétaire ne tienne pas de registre des personnes utilisant ses prestations, et que l'un des clients télécharge[29] de la musique illégalement sur des réseaux peer-to-peer. Il sera difficile de prouver qui était le client responsable de ce délit, et il sera beaucoup plus simple de se retourner contre le propriétaire de l'établissement. De même, envisageons le cas où une personne veuille accéder, sur la base de la législation sur les données à caractère personnel, aux données qui le concernent et qui sont traitées par son fournisseur d'accès. Il lui sera difficile de prouver qu'il est bien la personne à laquelle se rapportent les données.

En tout état de cause, ces problèmes peuvent être évités par la mise en place d'un présomption simple de la qualité d'internaute en faveur de l'abonné. Cette présomption pourra être combattue par l'abonné chaque fois que sa responsabilité sera engagée, par tout moyen. Ainsi si un client réalise des actes délictueux à partir des postes informatiques de son cybercafé, le propriétaire abonné pourra prouver quel client utilisait le poste à des dates et heures exactes et précises. De même la présomption pourra être mise en défaut par l'utilisateur lorsqu'il voudra faire jouer ses droits ou défendre sa personne. Il lui suffira de prouver qu'il a subi l'atteinte afin de pouvoir bénéficier des prérogatives offertes par chaque législation.

35. A notre sens, la conception de l'internaute comme abonné ne rend pas compte de la situation réelle de l'utilisation de l'Internet, et ce malgré le lien qui unit certaines données de connexion à sa personne. Nous opterons alors pour une conception extensive de l'internaute, que nous estimerons être tout utilisateur du réseau Internet. Conscients des problèmes probatoires que peut engendrer une telle conception, nous mettons également en avant un système efficace de présomption qui permet de ne pas avoir un tableau figé des différents intervenants. Cette présomption simple de la qualité d'internaute au bénéfice de l'abonné pourra être combattue simplement par lui-même lorsqu'on lui reprochera des faits qu'il n'a pas commis, mais pourra

[29] Téléchargement : Définition publiée par la Commission de l'informatique et des composants électroniques : Transfert de programmes ou de données d'un ordinateur vers un autre. Pour un internaute, le téléchargement est le plus souvent un transfert vers son propre ordinateur à partir d'un serveur, mais il peut avoir lieu dans l'autre sens.
Équivalent étranger 1 : downloading Note : Téléchargement à partir d'un autre ordinateur.
Équivalent étranger 2 : uploading Note : Téléchargement vers un autre ordinateur.

aussi être combattue par l'utilisateur non abonné qui voudra mettre en oeuvre ses prérogatives personnelles. Ainsi, chacun peut être en mesure d'exercer ses droits et de défendre ses intérêts.

La difficulté d'identification de l'internaute va essentiellement se retrouver lorsqu'il s'agira d'inclure ce dernier dans une législation, dans un régime juridique…

Section 2. L'internaute, une personne bénéficiant de protections juridiques

36. Une conception assez large de l'internaute ayant été posée, il convient à présent de se pencher sur les régimes juridiques dont il peut demander l'application. Deux régimes principaux s'offrent à l'internaute à travers ses données de connexion : d'une part il peut demander la protection de sa vie privée, que ce soit dans son intimité ou pour les correspondances qu'il émet par voie électronique, et d'autre part il peut requérir la protection de ses données de connexion en tant que données à caractère personnel.

§1. La vie privée de l'internaute

37. La vie privée est garantie à tous, cependant nous pouvons nous demander dans quelle mesure un internaute peut prétendre à la protection de celle-ci sur les réseaux mondiaux, si tant est qu'elle existe.

A. Le droit à la vie privée

38. Le droit à la vie privée se trouve présente dans de nombreux textes nationaux et internationaux. En France, ce droit fait l'objet de l'article 9 du Code civil. Le Conseil constitutionnel a estimé dans une décision du 23 juillet 1999 Couverture Maladie Universelle, que la vie privée se rattache à l'article 2 de la Déclaration des droits de l'Homme et du citoyen de 1789 qui pose le principe de la liberté personnelle.

Le terme de l'article 9 du Code civil « chacun » montre la volonté d'assurer à tous le droit à la vie privée. La qualité d'internaute reconnue à une personne n'enlève en rien la jouissance d'un tel droit. Un internaute pourra donc être protégé par le droit à la vie privée, et invoquer ce droit chaque fois qu'il en constatera une violation sur Internet.

Le droit pénal consacre par ailleurs un droit à la vie privée dans le domaine des télécommunications dans ses articles 226-1 et suivant.

Ces solutions semblent logiques dans la mesure où, lorsqu'il navigue sur Internet, l'internaute met sa vie privée à découvert : consultation de sites religieux, d'organisations syndicales, de mouvements politiques. L'Internet est aujourd'hui l'un des lieux dans lequel on révèle le plus l'intimité de sa vie privée et il semble indispensable de pouvoir se protéger par un outil tel que le droit à la vie privée.

B. Le droit à la correspondance privée

39. Le régime des correspondances émises par voie de télécommunication est régi par la loi n° 91-646 du 10 juillet 1991 qui pose un principe général de secret des correspondances émises par cette voie. Or les voies de télécommunications englobent, bien entendu, l'Internet au même titre que tous les réseaux informatiques. La loi de 1991 concerne donc aussi bien les opérateurs de télécommunications dites « classiques » telles que le téléphone ou les services postaux, que les opérateurs de télécommunications nés de l'avènement de l'Internet, comme par exemple les fournisseurs d'accès et les fournisseurs d'hébergement.

L'application du principe de secret des correspondances a été reconnu aux courriers électroniques par un jugement datant du 2 novembre 2000 de la 17ème chambre du Tribunal correctionnel de Paris qui a jugé que « *l'envoi de messages électroniques de personne à personne constitue de la correspondance privée* ».

L'internaute est donc bien protégé par le secret des correspondances privées lorsque les conditions requises par la loi de 1991 sont remplies c'est à dire qu'il existe une relation personnelle entre l'émetteur et le récepteur, mais aussi une relation personnelle entre l'objet du message et les personnes concernées. Cette solution a été reprise dans le jugement du Tribunal correctionnel précédemment cité qui dit que « *cette relation* (l'envoi de messages électroniques de personne à personne) *est protégée par la loi, dès lors que le contenu qu'elle véhicule est exclusivement destiné par une personne dénommée à une autre personne également individualisée, à la différence de messages mis à la disposition du public* ».

Enfin le secret des correspondances privées est garanti par des textes internationaux tels que l'article 8 de la Convention européenne des droits de l'homme qui assure le respect de sa correspondance à toute personne.

§2. Les données à caractère personnel de l'internaute

40. La protection des données à caractère personnel est récente dans l'histoire des droits de la personne. Cette garantie est soumise à des conditions strictes d'application : la donnée doit rendre une personne physique identifiée ou identifiable mais cette identification ne doit pas entraîner la mise en œuvre de moyens déraisonnés.

A. La donnée à caractère personnel doit rendre une personne physique identifiée ou identifiable

41. Selon l'article 4 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, « 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 ». Si l'on suit cet article, les personnes protégées par la loi de 1978 sont celles qui peuvent être identifiées par les informations nominatives.

Cette exigence se retrouve également dans l'article 2 de la directive 95/46/CE du 24 octobre 1995 concernant la protection des personnes physiques à l'égard du traitement automatisé des données à caractère personnel. En effet, cette disposition énonce que la donnée à caractère personnel est « *toute information concernant une personne physique identifiée ou identifiable ; est réputée identifiable une personne qui peut être identifiée, directement ou indirectement* […] ». Ainsi une donnée sera soumise à ce régime juridique non seulement si elle identifie une personne mais également si elle peut la rendre identifiable. Cela signifie qu'une conception de l'internaute comme tout utilisateur pourra se justifier au regard de la directive, car il sera quasiment toujours possible de remonter jusqu'à la personne visée par la donnée.

Cette potentialité d'identification est présente dans le projet de loi relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n°78-17 du 6 janvier relative à l'informatique, aux fichiers et aux libertés, dans son article 2. Cet article dispose que « *constitue une donnée à caractère personnel toute information relative à une personne physique identifiée ou qui peut être identifiée par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres* ». L'article ajoute que « *est la personne concernée par un traitement de données à caractère personnel celle à laquelle se*

rapportent les données qui font l'objet du traitement ». N'étant que la transposition des dispositions de la directive de 1995, ce projet de loi semble lui aussi admettre la possibilité de prendre en compte les utilisateurs d'Internet dans son dispositif de protection.

En pratique il sera parfois très difficile de déterminer la personne à laquelle les données de connexion se rattachent étant donné que la plupart du temps ces données permettront de ne remonter qu'à l'abonné. Mais comme nous l'avons examiné auparavant, il sera possible de remonter dans la quasi-totalité des espèces à la personne réellement visées par ces données.

Bien entendu, les difficultés d'application de ces dispositions varieront en pratique, notamment par rapport au principe de mise en œuvre raisonnable des moyens d'identification de la personne concernées par le traitement des données.

B. L'identification de la personne ne doit pas mettre en œuvre des moyens déraisonnés

42. Ce principe est inscrit dans le considérant 26 de la directive 95/46/CE du 24 octobre 1995 qui énonce que « pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens susceptibles d'être raisonnablement mis en œuvre, soit par le responsable du traitement, soit par une autre personne, pour identifier ladite personne ».

L'élément déterminant de ce considérant est la notion de mise en œuvre raisonnable, bien qu'aucune définition ni aucune illustration de celle-ci ne soient exposées. De plus, aucune décision de justice ne vient éclaircir l'étendue de la notion de mise en œuvre raisonnable. Il semble évident que ce concept sera appliqué au cas par cas, selon les circonstances de l'espèce.

Si l'utilisation de l'Internet se fait dans le domaine du foyer familial, alors il semble qu'il sera assez simple de déterminer quelle personne utilisait le terminal pour sa navigation. Imaginons que la conjointe de l'abonné au service veuille accéder à ces données à caractère personnel auprès du fournisseur d'accès à Internet, dans ce cas là il n'y aura pas de moyens déraisonnables à mettre en œuvre afin de déterminer si les données que sont les données de connexion font bien référence à elle. Ici, la théorie de l'internaute-utilisateur ne pose pas de grands obstacles à la mise en œuvre de la protection offerte par la législation sur les données à caractère personnel. En revanche, pourrait se poser une atteinte à la vie privée d'un autre membre de la famille si par exemple le conjoint accédait aux données de connexion de son épouse et qu'il découvrait qu'elle

navigue sur Internet à des périodes de la journée où elle est sensée travailler. De même, dans le cadre des cookies, il y aura peu d'aléas : si la personne a rempli un formulaire, alors son identification se fera sans aucun doute, mis à part le cas où une personne aurait usurpé son identité. Comme nous pouvons le constater, l'appréciation se fera *in concreto* par les juges.

En revanche, l'utilisation d'Internet dans les cybercafés, dans les entreprises et dans les universités peut engendrer de plus grandes difficultés. En effet, il pourra bien souvent apparaître irréalisable de déterminer une personne qui a utilisé Internet da ns un cybercafé. La tenue d'un registre sous forme électronique ou sous forme papier[30] peut comme nous l'avons vu être un moyen effectif de preuve de l'identité de l'internaute. Mais s'il n'y a aucune tenue de registre, on pourra considérer que la mise en œuvre des moyens d'identification de la personne pourra être appréciée comme déraisonnable.

Dans les entreprises et les universités, cette situation semble bien moins complexe : en entreprise les salariés disposent *a priori* de leur terminal et ont donc une adresse IP fixe propre ce qui rend aisée l'identification. Dans les universités, la situation est sensiblement la même étant donné que chacun des étudiants se voit en règle générale remettre un *login* et un mot de passe personnels. Là encore l'identification se fera simplement.

Dans la plupart des espèces, l'identification de la personne, que ce soit pour la poursuivre pour un délit, ou pour lui permettre de bénéficier de ses garanties légales, pourra se faire sans accroc. Toutefois cette appréciation du caractère raisonnable ou déraisonnable de la mise en œuvre des moyens d'identification de l'internaute restera à l'appréciation des juridictions. Il ne reste donc plus qu'à attendre les premières décisions.

[30] Registre qui constituerait un traitement de données à caractère personnel avec obligation de déclaration à la C.N.I.L.

Partie 2. L'accès aux données de connexion par l'internaute

43. Imaginons un internaute qui se connecte à Internet, comme chaque jour avec son ordinateur. Il lance sa connexion haut débit, son fournisseur d'accès lui attribue une adresse IP unique pendant la durée de sa connexion. Notre internaute lance son logiciel[31] de messagerie électronique : il reçoit 37 messages dont 28 non sollicités lui vantant, au choix, un moyen infaillible de gagner de l'argent, la rencontre avec l'âme sœur, ou encore la qualité de certains sites douteux… Loin d'être agacé, il en a l'habitude, l'internaute décide de consulter les nouvelles sur son site d'information favori : entre le moment où il ouvre son navigateur[32] et le moment où il accède à l'information qui l'intéresse, sept fenêtres pop-up s'ouvrent. Il lit quelques nouvelles puis décide d'acheter en ligne un ouvrage indispensable à ses études en économie : Le Capital de Karl Marx. Un tiers accède à son adresse IP, au document qu'il consulte et en déduit que notre ami est d'obédience communiste.

Sur un site traitant d'informatique, il découvre un nouveau *shareware*[33]. Il le télécharge pour l'essayer, le partagiciel contient un *spyware* qui étudie tout ce dont dispose l'internaute sur son disque dur et envoie les données à une société peu scrupuleuse.

---

[31] Logiciel : Définition publiée par l'arrêté du 22 décembre 1981 : Ensemble des programmes, procédés et règles, et éventuellement de la documentation, relatifs au fonctionnement d'un ensemble de traitement de données.

Équivalent étranger : software

[32] Navigateur : Définition publiée par la Commission de l'informatique et des composants électroniques le 13 mars 1999 : Dans un environnement de type Internet, logiciel qui permet à l'utilisateur de rechercher et de consulter des documents, et d'exploiter les liens hypertextuels qu'ils comportent.

Synonyme : navigateur, n.m.

Équivalent étranger : browser

[33] Shareware : Définition publiée par l'arrêté du 19 février 1993 : Logiciel mis à la disposition du public par son auteur, moyennant le versement d'une contribution en cas d'utilisation effective.

Ceci n'est qu'un exemple de ce que les internautes risquent chaque jour lors de leurs voyages virtuels. Ce que peut subir l'internaute peut aller bien au-delà de cette illustration.

L'internaute, bien qu'il n'en ait pas conscience, doit savoir quelles sont les attaques dont il peut faire l'objet en accédant à ses propres données de connexion (Chapitre 1). De cet accès il pourra parfois constater que des infractions sont commises à son encontre. L'internaute pourra alors avoir la nécessité d'accéder aux données de connexion de tiers (Chapitre 2).

Chapitre 1. L'accès de l'internaute aux données de connexion le concernant

44. Les raisons de l'internaute pour accéder aux données dont il fait l'objet peuvent être multiples : pressentiment d'une atteinte à sa vie privée ou encore simple curiosité peuvent en faire partie.

En pratique, l'accès par l'internaute à ses données de connexion est peu pratiqué. Ceci peut être dû au fait que l'internaute n'a pas toujours conscience des risques encourus de par son utilisation d'Internet.

Il n'en demeure pas moins qu'il peut être nécessaire pour un internaute d'accéder à ses données de connexion afin de savoir ce qu'il en advient.

L'internaute pourra accéder aux données de connexion le concernant au moyen de deux types de législations. La protection de sa vie privée pourra nécessiter que le juge accorde à l'internaute l'accès aux données de connexion dont il fait l'objet (section 1).

Mais l'accès le plus fréquent de l'internaute à ses données de connexion se fera par le biais de la législation sur les données à caractère personnel, qui prévoit et encadre parfaitement cet accès (section 2).

Section 1. L'accès de l'internaute à ses propres données de connexion au regard de la législation protégeant sa vie privée

45. La vie privée des internautes est constamment mise en péril sur le réseau Internet. Il est en effet très facile de suivre un internaute pendant sa navigation, de savoir quels sites et quels documents il consulte. Il est aussi possible de connaître ses contacts, et les échanges qu'il a avec eux. Les internautes n'ont pas souvent conscience que de telles atteintes à leur égard sont perpétrées.

§1. L'accès de l'internaute aux données le concernant au moyen du droit à la vie privée proprement dit

46. Actuellement, les moyens de surveiller les internautes sont nombreux et relativement faciles à mettre en œuvre que ce soit pour un particulier ayant de bonnes bases informatiques ou pour un professionnel. L'internaute est ainsi mis à nu sur le réseau quelles que soient ses activités : *chat*, participation à des forii, visite de sites commerciaux ou non… Les atteintes peuvent se faire par son adresse IP ou par les cookies, sans qu'il n'en ait aucun soupçon.

L'internaute qui subit une atteinte à sa vie privée pourra saisir le juge afin de la faire cesser, mais il faut savoir qu'en matière informatique, en apporter la preuve serait assez difficile. Dans ce cas il pourra se tourner vers la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

Il sera toutefois possible pour les internautes méfiants de vérifier qu'il n'est commis aucune intrusion dans sa vie privée en demandant aux personnes soupçonnées si elles traitent ses données. Il devra alors avoir recours à la législation sur les données à caractère personnel afin de savoir si des données le concernant font l'objet d'un traitement, et le cas échéant de savoir quelles données sont visées.

§2. L'accès de l'internaute aux données le concernant au moyen du droit au secret de ses correspondances

47. En ce qui concerne les correspondances de l'internaute le principe est le même que pour la protection de sa vie privée. Il est assez simple, en l'absence de moyens de cryptage, de savoir ce que contiennent les courriers électroniques envoyés et reçus par l'internaute. De plus, les fournisseurs d'accès à Internet offrent très souvent un service de courrier électronique et il pourrait leur venir à l'idée d'observer le courrier de leurs abonnés. Par exemple, Google le fait avec son service Gmail : des robots scrutent les messages des usagers afin de leur proposer des publicités ciblées sur les mots contenus dans le message.

L'internaute pourra décider de passer par le juge pour faire cesser toute atteinte relative au secret de ses correspondances. Et il disposera encore de la possibilité de mettre en jeu le droit des informations nominatives et des données personnelles afin de savoir si des données sont traitées par les personnes soupçonnées et comment.

48. L'internaute doit donc savoir s'il existe des atteintes à sa vie privée par deux moyens : soit il en est certain et saisit le juge, soit il n'en est pas sûr et utilise la loi de 1978 et la directive du 24 octobre 1995. L'utilisation de la législation sur les données à caractère personnel se justifie pleinement dans le cadre de la protection de la vie privée. En effet, la protection des données à caractère personnel fait partie de la protection de la vie privée. L'article 1 de la loi du 6 janvier 1978 y fait référence en disposant que l'informatique ne doit pas porter atteinte à la vie privée.

Section 2. L'accès de l'internaute à ses propres données de connexion au regard du droit de la protection des données à caractère personnel

49. La législation sur les données à caractère personnel donne de grandes prérogatives aux personnes concernées par des traitements de données les concernant. La loi n° 78-17 du 6 janvier 1978 a donné un élan à l'essor de cette législation, et a été reprise en partie lors de l'élaboration de la directive 95/46/CE du 24 octobre 1995. Ces textes contiennent à quelques nuances près les mêmes dispositions et offrent donc des garanties équivalentes aux citoyens.

Les internautes vont donc bénéficier de deux catégories de droits : d'une part des droits permettant l'accès aux données traitées, et d'autre part des droits qui font suite à l'existence d'un traitement de données à caractère personnel. Ces droits vont lui permettre de contrôler l'activité qu'il existe autour des informations qui le touchent.

§1. Les droits de l'internaute à accéder aux données à caractère personnel le concernant et faisant l'objet d'un traitement

50. Les droits qui permettent l'accès de l'internaute aux données le concernant qui font l'objet d'un traitement sont au nombre de deux. Le droit à la curiosité lui permet de savoir qu'il existe un traitement dont il fait l'objet, et le droit d'accès lui permet de savoir quelles données sont traitées.

A. Le droit à la curiosité

51. Le droit à la curiosité est régi par les articles 34 de la loi du 6 janvier 1978 qui dispose que « toute personne justifiant de son identité a le droit d'interroger les services ou organismes chargés de mettre en œuvre les traitements automatisés dont la liste est accessible au public en application de l'article 22 ci-dessus en vue de savoir si ces traitements portent sur des informations nominatives la concernant et, le cas échéant, d'en obtenir la communication ». Cette faculté est également offerte par la directive communautaire du 24 octobre 1995 dans son article 12 qui engage les Etats membres à garantir à toute personne concernée le droit d'obtenir du

responsable du traitement sans contrainte, à des intervalles raisonnables et sans délais ou frais excessifs la confirmation que des données la concernant sont ou ne sont pas traitées.

Ce droit permet à la personne qui soupçonne qu'un traitement est réalisé sur ses données à caractère personnel de savoir si ce supposé traitement est effectivement mis en œuvre ou non. L'exercice de ce droit n'est soumis à aucune condition. Ainsi l'internaute pourra dans tous les cas demander à son fournisseur d'accès, par exemple, si celui-ci réalise un traitement sur ses données. Et de la même manière, il pourra enjoindre le responsable d'un site Internet à lui révéler si ce dernier fait un traitement de ses informations nominatives à travers par exemple des cookies utilisés par ledit site. La seule restriction de ce droit est de ne pas en abuser, mais ceci paraît fort logique au regard de la théorie de l'abus de droit : l'internaute ne devra donc pas faire des demandes en nombre disproportionné.

Il pourra parfois apparaître difficile à l'internaute de justifier de sa qualité afin de connaître quelles sont les informations nominatives le concernant qui sont traitées. En ce qui concerne l'abonné qui veut exercer ce droit chez son fournisseur d'accès à Internet, ou chez son fournisseur d'hébergement, cela ne posera aucune difficulté puisqu'il pourra justifier de sa qualité aisément. Il en va de même lorsque l'internaute fera cette demande au responsable du site qui a traité ses cookies, dans lesquels ont été inscrits au moyen d'un formulaire ses coordonnées. En revanche, lorsque l'utilisateur, qui n'est pas l'abonné, voudra exercer ce droit chez les fournisseurs d'accès par exemple, la situation se dévoilera bien plus complexe. Il devra alors prouver qu'il est bien l'utilisateur de la connexion pendant un certain laps de temps. S'il arrive à apporter cette preuve, il pourra accéder aux données le concernant durant une période déterminée sur la connexion de l'abonné. Si tel n'est pas le cas, alors la présomption d'internaute jouera au bénéfice de l'abonné et l'utilisateur ne pourra accéder à ces informations.

En pratique, il apparaît toutefois que de nombreux internautes ignorent que des traitements de données à caractère personnel sont faits lorsqu'ils naviguent sur Internet, que ce soit les traitements opérés par leur fournisseur d'accès, par les responsables des sites qu'ils visitent, ou encore par leur hébergeur. Une information claire de la part de ces acteurs, qui expliquerait quelles données de connexion de ces internautes font l'objet d'un traitement, doit être faite afin de permettre aux utilisateurs d'Internet d'exercer leurs droits dans les meilleures conditions.

Lorsque le responsable du traitement a reçu la demande d'information, il doit fournir une réponse gratuite à l'internaute, sous peine d'une condamnation à une contravention de cinquième classe.

Déjà présent dans la législation française, le droit à la curiosité existe dans la loi de transposition de la directive 95/46/CE du 24 octobre 1995 à l'article 39. Cette disposition énonce que « *toute personne physique justifiant de son identité a le droit d'interroger le responsable du traitement de données à caractère personnel en vue d'obtenir la confirmation que des données le concernant font ou ne font pas l'objet de ce traitement* ». L'internaute devra ici justifier de son identité afin de savoir si des données le concernant sont traitées. Nous pouvons ajouter que dans certains cas, il devra également justifier de sa qualité d'internaute en démontrant qu'il était bien l'utilisateur du terminal pendant la période à laquelle il prétend que ses données à caractère personnel ont fait l'objet d'un traitement.

Une fois que l'internaute aura la confirmation que des données le concernant font l'objet d'un traitement, alors il pourra demander quelles sont ces données. C'est ici que sera mis en œuvre le droit d'accès.

B. Le droit d'accès aux données

52. Que ce soit dans la loi de 1978 ou dans la directive de 1995, le droit d'accès possède deux aspects. Ainsi, le droit d'accès peut être direct mais aussi indirect.

Le droit d'accès direct est régi par les articles 35 de la loi du 6 janvier 1978 et 12 de la directive du 24 octobre 1995.

L'article 34 dispose que « *le titulaire du droit d'accès peut obtenir communication des informations le concernant. La communication, en langage clair, doit être conforme au contenu des enregistrements* ». La définition du droit d'accès est sensiblement la même dans la directive qui offre à la personne concernée le droit de recevoir du responsable du traitement « *la communication, sous une forme intelligible, des données faisant l'objet des traitements, ainsi que toute information disponible sur l'origine des données* ».

Ce droit d'accès est un droit fondamental dans la législation sur les données à caractère personnel car c'est à partir de la connaissance des informations traitées que la personne concernée pourra exercer ses autres prérogatives.

Le droit d'accès exige ainsi que le responsable du traitement donne connaissance des informations à la personne concernée en langage clair, ou sous forme intelligible. Dans le cas de l'internaute, il arrivera fréquemment que les données de connexion lui soient totalement incompréhensibles. Lorsque le responsable du traitement sera la fournisseur d'accès à Internet, il devra tout mettre en œuvre pour que l'internaute puisse savoir de manière optimale à quelles dates et heures il s'est connecté. Si le responsable du traitement est le responsable d'un site, alors l'internaute devra être en mesure de comprendre quelles informations le concernant ont été enregistrées dans les témoins de connexion. Là encore, on peut supposer que l'internaute devra justifier de son identité et de sa qualité d'internaute afin d'accéder aux informations qui le concernent, de la même manière que dans le cadre de l'exercice du droit à la curiosité.

Des délais de réponse sont prévus par la loi en faveur du responsable du traitement : l'article 35 de la loi de 1978 énonce que la C.N.I.L. peut accorder des délais de réponse, suite à une procédure contradictoire. A l'issue de cette saisine, la C.N.I.L. a la faculté de dispenser le responsable du traitement à donner une réponse, lorsque les demandes sont abusives par leur nombre, par leur caractère répétitif ou systématique.

L'internaute pourra s'il le désire obtenir copie des enregistrements le concernant. Cette copie se fait sur papier, mais peut également se faire sur support électronique. L'internaute devra verser une redevance au responsable du traitement, dont le montant ne pourra être supérieur à un certain seuil. L'article 2 du décret du 23 décembre 1981 sanctionne un montant supérieur par une contravention de troisième classe.

Lorsque l'internaute demande l'accès aux données le concernant à un responsable d'un site Internet par exemple, ce dernier peut être tenté d'effacer ou de cacher les données. En effet, celui-ci a peut être porté atteinte à la vie privée de l'internaute en enregistrant des données de l'ordre de l'intimité de sa vie privée. Si l'internaute pressent ce risque, il pourra, conformément à l'article 35 de la loi de 1978 et à l'article 39 du projet de loi de transposition, demander au juge compétent d'ordonner toutes mesures de nature à éviter cette dissimulation ou cette disparition

d'informations. Cette demande peut se faire auprès du juge des référés, qui est le juge de l'urgence.

Ce droit d'accès est repris quasi identiquement dans l'article 39 du projet de loi de transposition de la directive de 1995.

Le droit d'accès indirect ne concerne que deux catégories de données : celles traitées dans le cadre de la sûreté de l'Etat et qui nous intéressent peu au regard de l'internaute, et celles se situant dans le domaine de la santé. Ces types de données n'ayant pas vocation à trouver leur place sur le réseau, elles n'auront pas être traitées dans le cadre des données de connexion de l'internaute.

§2. Les droits de l'internaute qui découlent de son droit d'accès

53. Une fois que l'internaute sait que des données nominatives sont traitées, il a la possibilité d'intervenir auprès du responsable du traitement. Il peut ainsi enjoindre ce responsable à corriger les informations qu'il traite. Mais il a également la possibilité de s'opposer au traitement même de ces données. Enfin il aura la possibilité de connaître la logique qui sous-tend le traitement.

A. Le droit de contester les informations et d'en obtenir la rectification

54. Le premier droit offert à la personne concernée par un traitement de données à caractère personnel est celui de pouvoir contester ces informations et d'en demander la rectification. Ce droit est prévu par les textes : la loi du 6 janvier 1978 l'envisage dans son article 36 et la directive du 24 octobre 1995 dans son article 12. La directive est moins précise que la loi de 1978 : alors que le texte communautaire envisage ce droit dans le cas de données incomplètes ou inexactes, la loi française implique les informations qui sont inexactes, incomplètes, équivoques, périmées ou dont la collecte ou l'utilisation, la communication ou la conservation est interdite. Le projet de loi de transposition de la directive de 1995 en droit français reprend la terminologie de la loi de 1978 dans son article 40.

Dans le cadre de l'Internet, des données pourraient être traitées de manière incomplète lorsque le fournisseur d'accès n'enregistre que les heures de connexion sans les dates. De même les données seront inexactes lorsque le fournisseur d'accès aura attribué dans ses fichiers de données de connexion la mauvaise adresse IP au mauvais login, ou lorsqu'il n'enregistrera pas des dates et heures de connexion précises et exactes. Le cas de la donnée périmée peut aussi être intéressant. Il est probable qu'un changement de titulaire du contrat d'abonnement au service fourni par l'opérateur d'accès à Internet surviendra. Si le fournisseur d'accès ne change pas les coordonnées de l'ancien abonné par celle du nouveau, alors les données enregistrées ne seront pas valables du fait de l'absence de mise-à-jour. En ce qui concerne les cookies, les données peuvent aussi être inexactes ou incomplètes, ou encore périmées.

Lorsque la personne concernée aura découvert que les informations se rapportant à sa personne ne sont pas exactes ou complètes, il sera en droit de les contester et d'en demander la rectification. La loi de 1978 permet au titulaire du droit d'accès d'exiger que les données soient rectifiées, complétées, clarifiées, mises à jour ou encore effacées. Cette énonciation est reprise fidèlement par le projet de loi de transposition de la directive. Pourtant, la directive se montre moins démonstrative en permettant au titulaire du droit d'accès d'obtenir du responsable du traitement la rectification, l'effacement ou le verrouillage des données.

Le responsable du traitement, quel qu'il soit (fournisseur d'accès ou d'hébergement, responsable d'un site), devra remplir cette obligation de rectification au risque d'encourir une contravention de cinquième classe prévue par le décret du 23 décembre 1981.

Une fois que l'internaute aura fait sa demande de rectification, deux situations peuvent se présenter. Tout d'abord, le responsable du traitement peut rectifier ou supprimer les données sans résistance. Cette situation ne pose aucun problème en pratique, c'est un arrangement à l'amiable. Toutefois, il semble évident que l'internaute ne pourra pas demander au fournisseur d'accès à Internet de supprimer les données de connexion le concernant, car celles-ci ont une finalité précise qui est la facturation ainsi que la conservation à des fins judiciaires. Dans le cas des données de connexion collectées par le fournisseur d'accès dans le domaine de son activité d'accès à Internet ou d'hébergement, l'internaute ne pourra ainsi demander que la modification des données, lorsque celle-ci sera opportune. En revanche, pour les cookies, il n'y a aucune

restriction : si l'internaute juge que les données doivent être effacées et que le responsable du site Internet accède à cette demande, aucune disposition légale n'interviendra pour interdire.

Le second cas concerne le refus du responsable du traitement à accéder à la demande du titulaire du droit d'accès au motif qu'il considère cette information comme exacte par exemple. Dans ce conflit, la charge de la preuve incombera au responsable du traitement sauf « *lorsqu'il est établi que les informations contestées ont été communiquées par la personne concernée ou avec son accord* ». Ce renversement de la charge de la preuve, prévue à l'article 36 de la loi de 1978, pourrait faire expressément référence aux cookies contenant des informations que l'internaute aurait données par le biais d'un formulaire. Dans une telle espèce, l'internaute devra alors prouver que les informations qu'il a fournies sont erronées.

Lorsque la demande de rectification a abouti, l'article 12 de la directive permet à la personne concernée de demander au responsable du traitement de notifier la modification, la suppression ou le verrouillage des informations aux tiers auxquels ces informations ont été communiquées. La condition de cette notification est que cette notification ne soit pas impossible ou suppose des efforts disproportionnés. L'article 38 de la loi de 1978 prévoit également une règle similaire.

L'internaute pourra obtenir copie de l'enregistrement modifié et ce, gratuitement. Lorsqu'il a été procédé à des modifications sur les informations le concernant et dont l'internaute avait demandé l'accès, alors la redevance payée au titre de ce droit d'accès devra lui être totalement remboursée.

B. Le droit d'opposition au traitement

55. L'internaute a la possibilité de s'opposer à ce qu'un traitement de ces données à caractère personnel soit opéré. Cette prérogative est prévue à l'article 26 de la loi de 1978 qui dispose que « *toute personne physique a le droit de s'opposer, pour des raisons légitimes, à ce que des informations nominatives la concernant fassent l'objet d'un traitement* ». Le droit communautaire reprend cette disposition à l'article 14 de la directive qui dit que « *les Etats membres reconnaissent à la personne concernée le droit de s'opposer à tout moment, pour des raisons prépondérantes et légitimes tenant à sa situation particulière, à ce que des données la concernant fassent l'objet d'un traitement* ».

L'internaute pourra ainsi à tout moment demander l'arrêt d'un traitement ayant pour objet des données le concernant à condition qu'il justifie de raisons légitimes selon la loi de 1978, ou de raisons légitimes et prépondérantes tenant à sa situation particulière selon la directive de 1995. Il apparaît difficile de délimiter cette notion de raison légitime, étant donné que la loi n'en donne aucune définition et que le contentieux en la matière est inexistant. La raison légitime devra être appréciée par les responsables du traitement *in concreto*, et le cas échéant, par les juges. Ainsi un internaute qui s'opposera au traitement réalisé par son fournisseur d'hébergement ou d'accès à Internet, obligera ce dernier à arrêter de lui fournir l'accès au réseau. S'il veut continuer de profiter de son accès à Internet auprès de ce fournisseur d'accès, l'internaute devrait alors amener une raison légitime qui surpassera les fins de facturation et de conservation judiciaire des données. Une telle raison sera en l'espèce impossible à rapporter. Le droit d'opposition dans les relations avec le fournisseur d'accès est *a priori* irréalisable. Néanmoins, pour l'internaute assailli par les cookies de toutes sortes, notamment ceux contenant des informations le concernant personnellement, il sera relativement aisé d'apporter un intérêt légitime afin de faire cesser le traitement par le responsable du site Internet et d'en obtenir la suppression. Dans le cas où les cookies contiendraient des données à caractère personnel à l'insu de l'internaute, il pourra arguer de son droit à la tranquillité afin de faire cesser le traitement.

Il est à noter que le projet de loi de transposition ne fait pas référence qu'à la notion de raison légitime et ne vise pas le texte de la directive de 1995 et sa « *raison légitime et prépondérante* ».

La directive ajoute que lorsque le traitement se fait à des fins de prospection, le titulaire du droit d'accès peut s'y opposer de manière gratuite.

Le code pénal sanctionne très durement le non respect de ce droit d'opposition offert à l'internaute titulaire du droit d'accès : l'article 226-18 punit de cinq ans d'emprisonnement et de 300 000 euros d'amende le fait, par le responsable du traitement, de procéder à un traitement d'informations nominatives concernant une personne physique malgré son opposition, fondée sur des raisons légitimes.

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

56. Ce droit se situe à l'article 3 de la loi de 1978 et à l'article 12 de la directive de 1995. La directive permet à l'internaute de d'obtenir de la part du responsable du traitement la

connaissance de la logique qui sous-tend le traitement automatisé des données qui le concerne « *au moins dans le cas des décisions automatisées visées à l'article 15 paragraphe 1* ». 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. Ce droit à connaître la logique qui sous-tend le traitement est évidemment repris dans le projet de loi de transposition. L'article 39 énonce ainsi que le titulaire du droit d'accès peut obtenir du responsable du traitement les informations permettant de connaître et de contester la logique qui sous-tend le traitement automatisé lorsque les résultats de celui-ci lui sont opposés.

En l'espèce, lorsque l'internaute exercera ce droit auprès des personnes qui traitent des données le concernant, il devra savoir à quoi servent ces données. Le fournisseur d'accès pourra facilement justifier la logique du traitement en ce qui concerne la facturation ou la conservation légale. En revanche, si celui-ci utilise les données dans un but autre que ceux-ci, il pourrait lui sembler dommageable de révéler la logique, notamment dans le cas dans lesquels les informations auront servi de base à une décision concernant l'internaute. La décision peut être celle de résilier le contrat de l'internaute en cas d'utilisation intensive de son accès et notamment des débits offerts. Nous pouvons citer le cas d'internautes qui téléchargent et envoient un nombre important de fichiers volumineux (de manière légale) par le réseau. De cette intense activité résulte un coup non négligeable pour l'opérateur et celui-ci serait tenté d'obtenir le départ de l'internaute par tous les moyens, y compris en mettant fin à leurs relations contractuelles. Une telle décision entrerait dans le champ d'application des articles 12 de la directive et 3 de la loi française. L'internaute serait alors en mesure de demander dans quelle logique les données se rapportant à lui ont été utilisées. Pour les fournisseurs d'hébergement, le problème peut être sensiblement le même. Ceux-ci sont souvent tentés de mettre fin à l'hébergement des pages dont le succès est grand, car ce succès se traduit par un nombre important de visites. Autant de visites qui consomment une grande part de bande passante, source de coûts supplémentaires pour l'hébergeur. A ce moment, le traitement des données sert de base à la décision.

Le responsable d'un site Internet pourra lui aussi être amené à dévoiler la logique qui sous-tend le traitement des données à caractère personnel qu'il opère par la gestion des cookies. Cette logique peut être une logique de recensement mais aussi de traçage. Ainsi un site de commerce en ligne pourra connaître les goûts d'un internaute en matière cinématographique et l'orienter vers les

articles les plus susceptibles de l'intéresser. Un tel profilage pourrait être perçu comme une atteinte à la vie privée.

Dans tous les cas, l'internaute pourra faire jouer le droit des données à caractère personnel afin de connaître quelle logique sous-tend le traitement. Si la logique lui semble contestable, il pourra alors faire valoir ses arguments auprès de la personne concernée, en vertu de l'article 15 de la directive de 1995, pour garantir la sauvegarde de son intérêt légitime. Nous pouvons même imaginer que dans le cas de rupture de contrat par le fournisseur d'accès pour utilisation intensive de la connexion, ou par le fournisseur d'hébergement pour trop grande consommation de bande passante, l'internaute puisse ester en justice pour rupture abusive de la convention.

Chapitre 2. L'accès de l'internaute aux données de connexion de tiers

57. Tout comme il peut avoir besoin de savoir ce qu'il est fait avec ses données de connexion, l'internaute peut avoir besoin d'accéder aux données de connexion de tiers. Les raisons de cet accès peuvent être nombreuses et la plus légitime sera le fait pour l'internaute de subir des infractions à travers le réseau.

Les infractions pouvant être commises envers l'internaute par Internet sont bien plus nombreuses que ce que l'on peut imaginer. Les infractions peuvent porter sur la personne même de l'internaute, voire sur ses biens, ou encore sur la jouissance de son utilisation d'Internet.

Les atteintes les plus importantes seront assurément celles qui portent sur les droits de la personnalité offerts à l'internaute, que ce soit au niveau de sa vie privée ou encore au regard de la protection de ses données personnelles… (section 1). Nous verrons que l'internaute bénéficie d'un véritable arsenal juridique afin de défendre sa personne et les données qui le concerne.

Les biens, matériels ou immatériels, de l'internaute pourront subir des attaques de la part de personnes mal intentionnées, et l'internaute sera parfois contraint d'engager les moyens juridiques de défense les plus sévères (section 2).

Les atteintes les plus nombreuses seront celles qui toucheront sa tranquillité : pop-up, spamming[34], spywares, cookies… Ceci se produit quotidiennement, même si ce ne sont pas les atteintes les plus graves (section 3).

Si l'internaute bénéficie toujours d'une protection appropriée, la pratique du contentieux montre que celui-ci n'utilise pas assez les moyens mis à sa disposition.

[34] Spamming : Définition publiée par la Commission de l'informatique et des composants électroniques le 1er septembre 2000 : Envoi d'un même message électronique à un très grand nombre de destinataires au risque de les importuner. Un exemple est l'envoi de messages publicitaires.

Piratages informatiques, contrefaçons à distance, pratiques commerciales déloyales, violations de la vie privée, profilage… Internet est-il devenu un lieu peu fréquentable ?

Section 1. L'accès aux données de connexion de tiers suite à une atteinte à la personne de l'internaute

58. Lors de ses navigations sur Internet, l'internaute met régulièrement sa personne à nue. En effet, les traces de l'internaute sur le réseau permettent de savoir quels sont ses goûts littéraires, cinématographiques ou musicaux mais aussi de savoir quelles peuvent être ses orientations politiques, sexuelles, religieuses, philosophiques ou syndicalistes. Il devient alors très tentant pour certains tiers de connaître les préférences de l'internaute, que ce soit à des fins publicitaires ou à des fins de profilage.

Afin de prévenir et de sanctionner ces attaques, l'internaute dispose d'un véritable arsenal juridique : d'une part il peut actionner le mécanisme commun de la protection de la vie privée au civil comme au pénal, et d'autre part il dispose de la protection de ses données à caractère personnel.

§1. Les atteintes aux données à caractère personnel de l'internaute

59. L'internaute subit régulièrement des atteintes par rapport aux données de connexion qu'il laisse sur le réseau. Des tiers peuvent, comme nous l'avons étudié, collecter des données et opérer des traitements de celles-ci sans que l'internaute ne s'en doute. D'autres atteintes peuvent survenir au regard de la protection des données à caractère personnel, lorsque le responsable du traitement fait un détournement de la finalité du traitement ou encore lorsqu'il les conserve à une durée supérieure à celle prévue. Il existe pourtant des moyens de défense mis à la disposition des personnes concernées. Ce dispositif de défense a une valeur forte et permet de pouvoir obtenir des sanctions sévères à l'égard des responsables de traitement malveillants.

A. La conservation des données au-delà de la durée de conservation

60. Les données de connexion de l'internaute ne doivent être conservées que le temps de la réalisation de la finalité pour laquelle elles ont été collectées. Cette restriction de la durée de conservation des données de connexion est prévue par l'article 5,1° de la loi 2000-321 du 12 avril 2000 qui modifie l'article 28 de la loi du 6 janvier 1978. L'article 28 dispose en effet que la durée

de conservation des informations collectées ou traitées sous forme nominative ne peut excéder la durée nécessaire à la réalisation des finalités, pour lesquelles ont été opérés ces collectes ou traitements, que dans le cas de fins historiques, statistiques ou scientifiques.

La directive de 1995 a repris cette règle en son article 6-1e) : « *Les Etats membres prévoient que les données à caractère personnel doivent être conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont collectées ou pour lesquelles elles sont traitées ultérieurement. Les Etats membres prévoient des garanties appropriées pour les données à caractère personnel qui sont conservées au-delà de la période précitée, à des fins historiques, statistiques ou scientifiques* ». Le projet de loi de transposition de la directive en France reprend ce principe dans son article 6-5.

Dans leur déclaration de traitement d'information nominative auprès de la C.N.I.L., les opérateurs devront définir une durée nécessaire de conservation pour la réalisation des finalités du traitement. Cependant, la durée fixée par les responsables du traitement peut être considérée comme excessive comparativement aux fins du traitement. Ils devront donc aussi exposer les finalités du traitement de manière extrêmement précise car, en cas de contestation, l'interprétation de la durée nécessaire à la conservation portera directement sur ces finalités.

Les fournisseurs d'accès à Internet, les fournisseurs d'hébergement et les responsables de sites auront alors intérêt à fixer la durée de conservation de manière raisonnable car la sanction encourue peut être très lourde. L'article 226-20, dont la modification résulte de la loi du 12 avril 2000, dispose que le fait de conserver, hors des cas de conservation à fins historiques, statistiques ou scientifiques, des informations sous une forme nominative au-delà de la durée prévue par le demande d'avis ou la déclaration préalable à la mise en œuvre du traitement informatisé est puni de trois ans d'emprisonnement et d'une amende de 45 000 euros. Le texte punit également des mêmes peines le traitement des données conservées au-delà de la durée de conservation contenue dans la demande d'avis ou dans la déclaration préalable.

En outre, les responsables de traitement des données de connexion de l'internaute seront aussi soumis à des lois spéciales qui imposeront des durées maximales de conservation de ces informations dans certains domaines. Ces régimes particuliers de conservation seront analysés lors de l'étude des obligations auxquelles sont soumis les responsables de traitement lorsqu'ils

font des traitements automatisés de données à caractère personnel sur la base des données de connexion de l'internaute (voir n°).

B. La collecte et le traitement frauduleux ou déloyaux

61. La collecte par moyen frauduleux, déloyal ou illicite consiste en le fait de collecter les données de connexion de l'internaute par des moyens détournés. En principe, l'internaute dont les données sont collectées doit donner son consentement préalable à la collecte et au traitement, tel qu'il est prévu par la directive du 24 octobre 1995 dans son article 7 qui dispose que le traitement de données à caractère personnel ne peut être effectué que si la personne concernée a indubitablement donné son consentement. La loi de 1978 n'avait pas envisagé un tel principe, mais le projet de loi de transposition devra comprendre cette disposition. Pour le fournisseur d'accès, que ce soit dans l'exercice de la fourniture d'un accès à Internet, ou que ce soit dans la fourniture d'hébergement, cette obligation pourra ne pas être remplie. En effet, l'article prévoit des exceptions au principe de consentement préalable, notamment lorsque le traitement de données à caractère personnel est nécessaire à la réalisation de l'intérêt légitime poursuivi par le responsable du traitement. Le fournisseur d'accès pourra facilement apporter la preuve que la collecte et le traitement des données de connexion de l'internaute sont nécessaires à la fourniture du service ainsi qu'aux fins de facturation. En revanche, nous pouvons concevoir que l'internaute subisse régulièrement des collectes de données à caractère personnel lorsqu'il visite des sites Internet ou lorsqu'il télécharge des fichiers sur les réseaux peer-to-peer. Le responsable du site Internet pourra ainsi récupérer des informations concernant les habitudes de l'internaute par la biais des cookies. Sur les réseaux peer-to-peer, l'adresse IP de l'internaute est visible par tous et on peut penser que des personnes soient très intéressées de savoir quels sont les fichiers téléchargés par les internautes. L'internaute pourra agir contre les collectes faites par moyen frauduleux.

C. Le détournement de finalité du traitement

62. Le détournement de finalité est consacré par l'article 226-21 du code pénal. Cet article punit « le fait, par toute personne détentrice d'informations nominatives à l'occasion de leur enregistrement, de leur classement, de leur transmission ou de toute autre forme de traitement, de

détourner ces informations de leur finalité telle que définie par la disposition législative ou l'acte réglementaire autorisant le traitement automatisé, « ou par la décision de la Commission nationale de l'informatique et des libertés autorisant un traitement automatisé ayant pour fin la recherche dans le domaine de la santé, » ou par les déclarations préalables à la mise en œuvre de ce traitement, est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende ».

Le code pénal envisage ici toutes les situations, que le traitement ait fait l'objet d'un régime d'autorisation ou d'un régime de simple déclaration préalable. Dans le cas des opérateurs de l'Internet, a priori les traitements des données de connexion doivent faire l'objet d'une déclaration préalable en vertu de l'article 16 de la loi de 1978.

Ainsi les opérateurs de l'Internet devront respecter la finalité exposée dans la déclaration préalable faite à la C.N.I.L.. Le fournisseur d'accès devra ainsi justifier le traitement des données de connexion de l'internaute par les nécessités de la fourniture du service, ainsi que par les fins de facturation. La situation sera la même pour le fournisseur d'hébergement, qui devra traiter ces données afin d'assurer l'exercice de son activité. Le responsable du traitement des données de connexion opéré par les cookies, devra lui aussi exposer une finalité à ce traitement. Les motifs peuvent être divers : accès à certaines informations par *login* et mot de passe, *mailing-list*, accès personnalisé au site web… Il ne devra pas se détourner de ces finalités, sous peine d'encourir des sanctions civiles et pénales. Or en pratique, la tentation d'utiliser les données de connexion des internautes à des fins autres que celles contenues dans la déclaration préalable peut être très grande. Ainsi le responsable du site pourrait vouloir profiler ses visiteurs par le biais des témoins de connexion. Ceci lui permettrait notamment de proposer des publicités en rapport avec les goûts des internautes. Imaginons qu'un disquaire en ligne cerne les préférences d'un internaute donné, et lui propose par la suite des disques d'un même genre. Il pourrait s'agir ici d'un détournement de finalité : le but à l'origine du traitement des données était de proposer un service de vente en ligne de disque, et les données sont en fait utilisées dans le but de cibler l'internaute.

Le fournisseur d'accès peut aussi être tenté de découvrir les centres d'intérêts des internautes à qui il fournit l'accès à Internet. Le profilage des internautes pourrait ensuite être cédé moyennant finance à des tiers qui enverront la publicité adéquate sur les adresses de courrier électronique desdits internautes. Courrier électronique le plus souvent hébergé chez le fournisseur d'accès…

En cas de détournement de finalité, le responsable du traitement peut donc être puni très sévèrement par le droit pénal, en plus d'une condamnation civile.

Ce type d'atteinte aux données de connexion de l'internaute constitue la passerelle entre la violation de la protection des données à caractère personnel dont il bénéficie et la violation de sa vie privée. Dans la plupart des cas, l'atteinte à la vie privée de l'internaute pourra être commise par l'atteinte au respect de ses données à caractère personnel.

§2. Les atteintes à la vie privée de l'internaute

63. Lorsqu'une personne constate que sa vie privée a été violée, elle a la possibilité d'engager une action devant les juridictions civiles sur le fondement de l'article 9 du code civil. Ainsi, la personne demandera réparation par l'octroi de dommages et intérêts. Cette action a toutefois un caractère particulier, rappelé par l'arrêt de la première chambre civile de la Cour de cassation du 12 décembre 2000[35] : la victime n'a pas à prouver une faute et un préjudice particuliers car toute utilisation illicite d'un élément de la vie privée suffit à caractériser la violation de celle-ci.

Mais l'internaute aura aussi la possibilité de saisir le juge des référés afin de prendre toutes mesures afin de faire cesser l'atteinte.

De plus, quelques infractions relèvent du code pénal, il sera alors possible pour l'internaute d'engager la responsabilité pénale des personnes qui auront attenté à sa vie privée par le biais de ces données de connexion. Toutefois l'engagement de la responsabilité pénale du responsable du traitement des données de connexion ne pourra jouer que dans des cas limités.

A. Les atteintes à l'intimité de la vie privée de l'internaute

64. L'intimité de la vie privée de l'internaute est mise à rude épreuve sur les réseaux mondiaux. Si le code pénal envisage notamment l'enregistrement et la transmission de la parole et de l'image comme atteinte à la vie privée, il n'en demeure pas moins que d'autres atteintes plus courantes puissent être également constitutives de tel préjudice. Ainsi des infractions à la législation sur les informations nominatives mettront directement en péril la vie privée de

[35] Cass. civ. 1, 12/12/2000, Dalloz 2001, som. com. page 1987, obs. C. Caron

l'internaute, comme la divulgation des données de connexion à des tiers ou encore la collecte de données sensibles. Ceci peut sembler parfaitement logique dans la mesure où la loi du 6 janvier 1978 est une loi qui protège la vie privée.

1). L'enregistrement et la transmission de la parole et de l'image de l'internaute

65. L'article 226-1 du code pénal punit le fait de porter atteinte volontairement, par un quelconque procédé, à l'intimité de la vie d'autrui. Cet article concerne notamment la captation, l'enregistrement et la transmission, sans le consentement de la personne, des paroles que celle-ci a prononcé à titre privé ou confidentiel, ou de son image alors qu'elle se trouve dans un lieu privé.

Si cette disposition ne semble pas au premier abord entrer dans le cadre de la protection de la vie privée de l'internaute, il existe toutefois une situation à laquelle elle s'applique pleinement : l'audioconférence[36] et la visioconférence[37]. En effet, ces formes de communication se déroulent à travers le réseau Internet et permettent de converser avec son interlocuteur par la voix, ou par la voix et l'image pour peu que les intervenants disposent de webcams et des logiciels adéquats.

Si lors de cette audioconférence ou visioconférence, un tiers capte ou enregistre l'image ou la voix des internautes, alors celui-ci s'expose pleinement à la sanction prévue par le code pénal pour violation de l'intimité de la vie privée desdits internautes. En effet, les internautes se situeraient *a priori* dans un lieu privé, leur domicile, et s'échangeraient des propos à titre privé voire confidentiel.

---

[36] Audioconférence : Définition publiée par la Commission des télécommunications le 22 septembre 2000 : Téléconférence dans laquelle les participants sont reliés par des circuits téléphoniques qui permettent la transmission de la parole et éventuellement d'autres signaux tels que ceux de télécopie ou de téléécriture.

Équivalent étranger : audioconference

[37] Visioconférence : Définition publiée par la Commission des télécommunications le 22 septembre 2000 : Téléconférence permettant, en plus de la transmission de la parole et de documents graphiques, la transmission d'images animées des participants éloignés. On dit aussi « conférence vidéo ».

Synonyme : vidéoconférence

Équivalent étranger: videoconference, videophone conference

L'article prévoit une exception à cette prohibition lorsque les internautes ne sont pas opposés à ces actes alors qu'ils étaient en mesure de savoir qu'un tiers enregistrait, captait, fixait ou encore transmettait leurs images ou encore leurs paroles.

Hors cette situation, la personne qui a commis ces faits pourrait être condamnée à une peine d'un an d'emprisonnement et à une amende de 45 000 euros.

2). La divulgation des données touchant la vie privée à des tiers

66. La personne qui a recueilli des données à caractère personnel ayant trait à la vie privée des internautes ne peut les transmettre à des tiers qui n'ont pas qualité pour les recevoir lorsque la divulgation pourrait porter atteinte à la considération de cet internaute ou à sa vie privée. Cette règle est prévue par l'article 226-22 du code pénal qui punit ces faits d'une peine d'un an d'emprisonnement ainsi que d'une amende de 15 000 euros. Lorsque la faute aura été commise par imprudence ou par négligence, la peine d'amende se réduit à 7500 euros.

Le responsable du traitement des données de connexion, que ces données servent à connecter l'internaute au service ou à l'authentifier sur un serveur, ne pourra donc pas transmettre les habitudes de connexion des internautes dont il possède les données, lorsque cette divulgation peut porter atteinte à la vie privée ou à la considération de ceux-ci. Néanmoins, les internautes devront obligatoirement porter plainte afin que la poursuite ne soit exercée.

3). L'enregistrement de données sensibles

67. Les données sensibles sont les données à caractère personnel qui font apparaître directement ou indirectement les origines raciales ou les opinions politiques, philosophiques ou religieuses ou les appartenances syndicales ou les mœurs des personnes. Le traitement de ces données est interdit par la loi relative à l'informatique, aux fichiers et aux libertés de 1978 à l'article 31. L'article 8 de la directive de 1995 reprend cette règle en disposant que les traitements de données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, ainsi que le traitement des données relatives à la santé et à la vie sexuelle, sont interdits.

Sur le réseau, des transgressions à l'interdiction au traitement des données sensibles peuvent régulièrement se produire. Par exemple, le responsable d'un site de vente de produits culturels peut déduire à partir de la visite d'un internaute quelles sont ses orientations politiques, religieuses ou sexuelles. Il pourra savoir que tel internaute recherche des ouvrages traitant du libéralisme économique dans les civilisations occidentales, que tel autre a acheté des ouvrages d'obédience libérale, ou encore qu'un autre a passé commande pour l'édition prestige du Kama Sutra… Des profils des internautes pourront ainsi être établi au regard des ouvrages dont ils ont consulté la fiche ou alors que ceux-ci auront commandé. De tels profils seraient contraires à la loi de 1978.

Mais le fournisseur d'accès à Internet peut lui aussi avoir connaissance d'un grand nombre d'informations sur l'internaute. Par le biais des serveurs caches dont il a la charge, il lui est possible de savoir sur quels sites et quels documents a téléchargé l'internaute. Il pourrait alors savoir qu'un internaute a téléchargé l'édition en ligne de *Mein Kampf* et en déduire une orientation d'extrême droite, alors qu'il peut s'agir d'un étudiant en histoire des idées politiques qui fait des recherches.

Des exceptions existent à l'interdiction des traitements de données sensibles. Elles sont prévues aussi bien par la loi de 1978 que par la directive de 1995. Pour la loi de 1978, l'exception concerne les groupements politiques, religieux, philosophiques ou syndicaux qui ont la possibilité de tenir un registre de leurs membres et correspondants. Bien entendu l'interdiction ne jouera pas non plus en cas d'accord exprès de la part de l'internaute visé par le traitement automatisé. La directive de 1995 reprend ces exceptions et en ajoute de nouvelles : le traitement automatisé de données sensibles est réalisable lorsque nécessaire au respect du droit du travail, des intérêts vitaux de la personne, ou lorsque ces données ont été rendues publiques.

Lorsque le traitement ne fait pas l'objet du régime d'exception, le responsable du traitement encourt une peine de cinq années d'emprisonnement et de 300 000 euros d'amende, conformément à l'article 226-19 du code pénal.

B. Les atteintes à la correspondance privée de l'internaute

68. Le courrier électronique suscite de plus en plus la considération de la doctrine, notamment au regard de sa qualification de correspondance privée. A l'instar du courrier classique, le courrier

électronique peut facilement être intercepté. Les risques d'atteinte au courrier électronique ont été clairement exposées dans l'ouvrage de Mme Fenoll-Trousseau et M. Haas[38], avec pour ce qui nous intéresse le forçage des boîtes de courrier électronique, l'usurpation du mot de passe ou encore l'espionnage et autre risque de violation de la confidentialité. L'usurpation du mot du passe de la boîte de courrier électronique peut se faire de manière classique ou de manière électronique, et il pourrait en résulter un espionnage des correspondances privées échangées. Le forçage de la boîte sera en revanche des plus classiques : les auteurs prennent l'exemple du « *conjoint jaloux qui consulte la boîte électronique de sa moitié* ».

A notre sens il est évident que le courrier électronique doit être considéré comme de la correspondance privée, et ainsi être protégé comme tel par le secret. Pour être de la correspondance privée, le courrier électronique échangé doit remplir certaines conditions. Il doit exister une relation personnelle entre les deux correspondants, mais aussi une relation personnelle dans le contenu du message. Dès que ces caractéristiques sont présentes, le courrier électronique échangé est de la correspondance privée protégée par le secret. Le caractère privé du courrier électronique a été clairement admis par la jurisprudence, notamment par le jugement de la 17ème chambre du Tribunal correctionnel de Paris en date 2 novembre 2000[39] qui juge que *« l'envoi de messages électroniques de personne à personne constitue de la correspondance privée* » et que « *cette relation est protégée par la loi, dès lors que le contenu qu'elle véhicule est exclusivement destiné par une personne dénommée à une autre également individualisée, à la différence des messages mis à la disposition du public* ».

La Cour de cassation a également reconnu le caractère de correspondance privée au courrier électronique dans le secteur du travail et de l'entreprise, dans l'arrêt Nikon du 2 octobre 2001 (JCP, éd. E 2002).

Le courrier électronique, correspondance privée, est donc protégé par le secret des correspondances contenu dans la loi n° 91-646 du 10 juillet 1991. En plus des sanctions civiles, la personne qui commet des atteintes envers la correspondance privée de l'internaute risque également des sanctions pénales. Ces sanctions pénales sont prévues par l'article 226-15 qui punit d'une peine d'un an d'emprisonnement et de 45 000 euros d'amende « *le fait, commis de*

[38] Fennoll-Trousseau, M. et Haas, M. *Internet et protection des données personnelles.* Litec, 2000.

[39] TGI Paris, 17ème chambre correctionnel, décision du 2 novembre 2000, JCP éd. E 2002

mauvaise foi, d'ouvrir, de supprimer, de retarder ou de détourner des correspondances arrivées ou non à destination, et adressées à des tiers, ou d'en prendre frauduleusement connaissance ». L'article punit des mêmes peines l'interception, le détournement, l'utilisation ou la divulgation des correspondances émises, transmises ou reçues par la voie des télécommunications, « *ou de procéder à l'installation d'appareils conçus pour réaliser de telles interceptions* ».

Toutefois la loi du 10 juillet 1991 prévoit des cas dans lesquels le secret des correspondances est remis en question, en permettant des interceptions et des contrôles de courrier électronique lorsque celles-ci sont ordonnées par la voie judiciaire ou mises en œuvre sous l'autorisation écrite ou motivée du Premier ministre.

Dans les situations autres que celles prévues par ces exceptions l'internaute pourra agir devant les autorités judiciaires afin de faire procéder à la captation des données de connexion de l'internaute qui a attenté au secret de ses correspondances électroniques privées, afin d'engager des poursuites.

Section 2. Les atteintes aux biens de l'internaute

69. Sur Internet, ce n'est pas seulement par rapport aux traces qu'il laisse que l'internaute peut subir des atteintes. Des tiers malveillants ne se contentent pas de ses traces et peuvent en effet vouloir entrer directement dans la machine de l'internaute. Ces intrusions peuvent être commises pour un dessein déterminé comme contrefaire les droits de propriété intellectuelle de l'internaute ou profiter de ses investissements et travaux. Il peut y avoir intrusion aussi dans le seul but de consulter et de détruire des informations, ou encore pour placer un virus informatique.

Le droit offre des protections aux individus victime de telles intrusions. Tout d'abord, l'internaute bénéficie d'une protection de son ordinateur par le biais de la protection des systèmes de traitement automatisé de données prévue par le code pénal. Ensuite, ce sont les informations contenues sur ce système qui sont protégées, soit par la propriété intellectuelle, soit par des mécanismes communs de responsabilité civile.

§1. La protection du système informatique de l'internaute

70. La loi n° 88-19 du 5 janvier 1988 a introduit des dispositions nouvelles dans le code pénal du fait de l'apparition d'un nouveau genre d'infractions en matière informatique que l'on regroupe sous le vocable de cyber-criminalité. Cette loi avait pour but de protéger aussi bien la partie matérielle, l'unité centrale et les périphériques, que la partie immatérielle, le système d'exploitation et les logiciels, des systèmes de traitement automatisé de données. Ainsi, on va considérer que si une partie de l'ensemble est touchée, ce sera l'ensemble du système qui subira l'atteinte.

Aujourd'hui les dispositions de la loi du 5 janvier 1988 se retrouvent dans les articles 323-1 et suivants qui portent sur les atteintes aux systèmes de traitement automatisé de données. Ces articles prévoient un certain nombre d'infractions telles que l'accès et le maintien frauduleux dans le système de traitement automatisé de données, la modification du contenu du système, ou encore l'entrave au fonctionnement du système.

A. L'accès et le maintien dans la machine de l'internaute

71. L'accès et le maintien frauduleux sont prévu à l'article 323-1 du code pénal qui sanctionne le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données. Le code pénal ne sanctionne pas un accès et un maintien non frauduleux, c'est-à-dire par accident. Ainsi si un tiers se connecte accidentellement à l'ordinateur de l'internaute, et s'y maintient sans en avoir connaissance, alors ce tiers ne pourra être poursuivi sur le fondement de l'article 323-1 alinéa 1.

Concernant l'accès frauduleux, tous les modes d'intrusion dans l'ordinateur de l'internaute sont concernés, peu importe que la connexion se fasse à distance ou non. Il n'est pas non plus nécessaire que le tiers se trouve virtuellement dans le terminal de l'internaute, l'intrusion par un programme qui étudie les actions et le contenu de la machine est de la même manière sanctionnée par le code pénal.

Le maintien frauduleux à l'intérieur du système de traitement automatisé de données peut découler directement de l'accès frauduleux au système. Mais nous pouvons noter que le maintien frauduleux peut aussi résulter d'un accès régulier au système. Cela peut par exemple survenir dans le cas de certaines aides en ligne fournies par certains prestataires de services en ligne. Les fournisseurs d'accès à Internet ont ainsi très souvent des employés dont la fonction est d'aider les clients à résoudre leurs problèmes de connexion. De plus en plus, ces aides en ligne disposent du moyen de se connecter et de diriger la machine de l'internaute à distance. Cet accès est régulier puisque sollicité par l'internaute. Mais si une fois l'aide effectuée et les problèmes de connexion réglés, l'opérateur se maintient dans le système de l'internaute alors celui-ci commettra le délit de maintien frauduleux dans un système de traitement automatisé de données.

Le maintien frauduleux pourra aussi être commis par des personnes non sollicitées par l'internaute, que l'on surnomme « pirates[40] » ou « hackers [41]». Ceux-ci peuvent notamment

[40] Pirate : Définition publiée par la Commission de l'informatique et des composants électroniques le 16 mars 1999 : Personne qui contourne ou détruit les protections d'un logiciel, d'un ordinateur ou d'un réseau informatique.
Équivalent étranger : cracker

[41] Hacker : Définition publiée par la Commission de l'informatique et des composants électroniques le16 mars 1999 : Personne passionnée d'informatique qui, par jeu, curiosité, défi personnel ou par souci de notoriété, sonde, au hasard

s'introduire dans le système de l'internaute par le biais d'un *spyware* qui observera les faits et gestes de l'internaute et en rendra compte par la suite. Il est à noter que cette pratique n'est pas exclusive aux pirates en lignes, et que des sociétés connues ont tendance à avoir recours à ce genre de pratiques afin de surveiller les utilisateurs.

Les peines encourues par les personnes responsables de ces actes sont lourdes. En effet, le code pénal infligeait une peine d'un an d'emprisonnement et d'une amende de 15 000 euros à toutes personnes condamnées de ce chef. Aujourd'hui ces peines ont été revues à la hausse par loi du 21 juin 2004 sur la confiance en l'économie numérique : la peine d'emprisonnement sera de deux ans et l'amende est doublée, soit 30 000 euros.

L'alinéa 2 de l'article 323-1 envisage les conséquences de l'accès et du maintien frauduleux au système de traitement automatisé de données. Ainsi lorsque l'accès ou le maintien a eu pour conséquence soit de supprimer ou de modifier des données contenues dans le système, soit d'altérer le fonctionnement de ce système, les peines encourues sont doublées : la peine d'emprisonnement, depuis la loi de juin 2004, sera de 3 ans et l'amende de 45 000 euros. Nous pouvons constater que l'article de comporte aucune mention à l'ajout de données dans le système. Faut-il comprendre l'ajout dans le terme de modification ? De toutes évidences, l'ajout doit être considéré comme une conséquence de l'accès ou du maintien frauduleux dans le système. De la même manière, l'article ne comprend pas non plus le fait de copier des informations contenues dans le système : la copie n'est ni une modification ni une suppression des données. Du fait de l'interprétation stricte du droit pénal, la copie ne doit pas être comprise comme un acte condamnable.

B. L'entrave au fonctionnement de la machine de l'internaute

72. L'article 323-2 dispose que « *le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de trois ans d'emprisonnement et de 45 000 euros d'amende* ». Cette disposition concerne non seulement les personnes qui n'ont pas accès au système mais également celles-ci qui peuvent régulièrement y entrer. L'article envisage deux

---

plutôt qu'à l'aide de manuels techniques, les possibilités matérielles et logicielles des systèmes informatiques afin de pouvoir éventuellement s'y immiscer.

situations : d'une part l'entrave du fonctionnement et d'autre part le fait de fausser le fonctionnement.

Le fait d'entraver le fonctionnement du système signifie que le système ne pourra plus fonctionner et sera totalement bloqué. L'internaute connaîtra une entrave de son système lorsque celui-ci ne pourra plus l'utiliser en raison d'actes malveillants de la part d'un tiers.

Le fait de fausser le fonctionnement du système signifie que le système pourra continuer à fonctionner mais d'une manière anormale. Cet article permet de sanctionner les personnes qui envoient des virus informatiques ou encore des chevaux de Troyes dans les machines des internautes. Le virus ou le *trojan* auront souvent des effets néfastes sur l'ordinateur de l'internaute, comme un net ralentissement ou encore l'impossibilité d'utiliser certaines fonctionnalités du système d'exploitation ou d'un programme en particulier.

Il est à noter que les peines sanctionnant cette infraction ont aussi été augmentées : la peine d'emprisonnement est dorénavant de cinq années et l'amende de 75 000 euros.

C. L'ajout, la modification et la suppression de données contenues dans la machine de l'internaute

73. Le fait d'introduire frauduleusement des données dans un système de traitement automatisé de données ou de supprimer ou de modifier frauduleusement les données qu'il contient est puni par l'article 323-3.

L'article 323-3 s'applique aux personnes qui ont régulièrement accès au système. Dans le cas d'une telle atteinte au système de l'internaute, cette situation sera envisageable. En effet, s'il n'est pas fréquent que l'internaute accorde des accès à sa machine, certaines pratiques permettent de dire qu'un accès a été accordé à des tiers, notamment dans le cadre des réseaux peer-to-peer. La pratique des échanges sur ces réseaux suppose que chaque internaute permette aux autres d'accéder à une partie de son espace afin de pouvoir y prendre les fichiers disponibles et d'en envoyer. Cependant, la tentation peut être grande pour un pirate d'ajouter un fichier, tel un trojan ou un virus, afin de contaminer la machine de l'hôte. L'internaute pourrait alors se retourner contre ce tiers en le poursuivant pour ajout frauduleux de données dans son système. La solution serait la même lorsque l'invité sur l'ordinateur de l'internaute supprimerait les données contenues sur son disque dur.

Surviendront également des situations dans lesquelles l'internaute n'aura pas donné d'accès au contenu de sa machine. Malgré cela, les pirates en ligne sont tout à fait capables de s'introduire frauduleusement dans la machine de l'internaute et d'y ajouter, modifier ou supprimer des données.

Encore une fois, les sanctions risquées par les personnes accomplissant de tels actes sont lourdes puisque le code pénal envisageait une peine de trois années d'emprisonnement et d'une amende de 45 000 euros. Là encore, une hausse des peines est intervenues, avec une amende de 75 000 euros et une peine de prison de cinq années.

74. Le code pénal punit également la tentative de ces infractions des mêmes peines que celles de leur réalisation. La simple participation à un groupement formé dans le but de commettre ces infractions est aussi puni des mêmes peines que celles sanctionnant les infractions elles-mêmes. Des peines complémentaires sont ajoutées pour les personnes physiques : interdiction des droits civiques, civils et de famille pour une durée de cinq ans, interdiction d'exercer une fonction publique pendant cinq ans, confiscation du matériel qui a servi à l'infraction… Les personnes morales peuvent être déclarées responsables de ces infractions en vertu de l'article 323-6.

La loi du 21 juin 2004 sur la confiance en l'économie numérique a également inclus une nouvelle infraction à l'article 323-3-1 du code pénal. Il s'agit de l'infraction d'importation, de détention, d'offre, de cession ou de mise à disposition d'un équipement, d'un instrument, d'un programme informatique ou de toutes données conçus ou spécialement adaptés pour commettre une ou plusieurs atteintes aux systèmes de traitement automatisé de données prévues aux articles 323-1 et suivants du code pénal. Cette nouvelle infraction est réprimée des peines prévues pour l'atteinte elle-même ou pour l'infraction la plus durement sanctionnée.

§2. La protection des biens immatériels de l'internaute

75. L'internaute n'est pas toujours un utilisateur moyen, qui ne navigue sur Internet que pour ses loisirs. Il peut aussi être un artiste, par exemple un graphiste ou un musicien, ou encore un inventeur, qui se nourrit de ses brevets. De telles personnes peuvent posséder sur le disque dur de

leur ordinateur des créations représentant une véritable valeur économique, et des tiers pourront tenter de s'y introduire afin de copier ces créations.

Outre la protection des systèmes de traitement automatisé de données précédemment exposée, ces internautes bénéficient de régimes classiques de protection de leur propriété intellectuelle. Lorsque l'internaute ne disposera pas de droit de propriété intellectuelle, il pourra toutefois engager l'action en concurrence déloyale contre un concurrent.

A. La propriété intellectuelle comme moyen de défense

76. Le moyen de protection classique de la propriété intellectuelle est l'action en contrefaçon qui a une double nature civile et pénale, et une double fonction : c'est une action en revendication qui permet aussi d'obtenir réparation des préjudices causés.

L'internaute dont les créations présentes sur son disque dur sont contrefaites pourra demander au juge d'ordonner au fournisseur d'accès à Internet de donner les coordonnées de la personne qui s'est introduite dans la machine. Pour cela, le demandeur devra être soit le propriétaire, soit le cessionnaire, soit le licencié des droits conférés par la propriété intellectuelle. Ainsi, pour une œuvre de l'esprit protégée par le droit d'auteur, le cybernaute devra être l'auteur de l'œuvre musicale, littéraire, graphique ou encore logicielle contrefaite. Dans le cadre du brevet et de la marque, il devra être le déposant de la demande de brevet.

1). La protection de la propriété littéraire et artistique de l'internaute

77. Cette protection jouera lorsque l'internaute aura la qualité d'auteur afin de protéger les œuvres de son esprit.

L'internaute pourra se protéger contre tous ceux qui participent à la reproduction ou à la mise à disposition de l'œuvre contrefaisante au public. Ainsi il est fréquemment arrivé que des artistes musicaux voient leurs maquettes musicales mises à disposition des internautes des semaines avant la sortie officielle de leur œuvre. Il s'agit ici d'une atteinte manifeste au droit moral de divulgation de leur œuvre. Au pénal, l'internaute victime de cette contrefaçon devra prouver l'élément matériel et l'élément moral de l'infraction afin de faire condamner le tiers contrefaisant. Au civil, la mauvaise foi est indifférente.

L'auteur d'une telle contrefaçon encourt une peine sévère : d'une part il pourra être sanctionné par une obligation de verser des dommages et intérêts à l'auteur de l'œuvre, et d'autre part une peine de deux ans d'emprisonnement et une amende de 150 000 euros.

2). La protection de la propriété industrielle de l'internaute

78. Lorsque l'internaute sera un inventeur au sens du droit des brevets, c'est-à-dire qu'il aura déposé une demande de brevet devant l'Institut national de la propriété industrielle pour son invention, il pourra bénéficier de la protection de la propriété industrielle. Un internaute peut disposer des plans de son invention sur son ordinateur, et un tiers pourrait vouloir disposer de ces plans sans pour autant en faire la demande à l'INPI. S'il obtient les plans de l'inventeur, le tiers pourrait alors faire l'invention de manière optimale (ce que ne permettent toujours pas les documents déposés à l'INPI) et la mettre sur le marché.

Dans ce cas, le fait d'obtenir les données de connexion de l'internaute ayant pénétré la machine de l'inventeur importe peu puisqu'il suffit de prouver l'acte de contrefaçon qui consistera en l'atteinte au monopole du propriétaire du droit de propriété industrielle.

B. La concurrence déloyale comme moyen de défense

79. L'internaute pourra utiliser la concurrence déloyale pour protéger ses créations immatérielles lorsqu'il ne disposera pas sur celles-ci de droits de propriété intellectuelle.

La concurrence déloyale est une construction doctrinale et jurisprudentielle découlant des articles 1382 et 1383 du code civil.

L'article 1382 dispose que « *tout fait quelconque de l'homme, qui cause à autrui un dommage, oblige celui par la faute duquel il est arrivé, à le réparer* ». Selon l'article 1383, « *chacun est responsable du dommage qu'il a causé non seulement par son fait mais encore par sa négligence ou par son imprudence* ».

Ces dispositions ne permettent de faire jouer la concurrence déloyale qu'entre concurrents, et la faute doit être constituée par un acte déloyal comme notamment l'appropriation illicite d'un

investissement économique ou le fait d'utiliser les recherches d'autrui et de s'approprier son travail, ses efforts et son savoir-faire.

Un internaute qui a créé une invention mais qui ne l'a pas déposée pourra utiliser la concurrence déloyale lorsqu'un concurrent se sera introduit sur son terminal afin de « voler » son travail. L'internaute devra prouver la faute du tiers ainsi que le lien de causalité entre ce fait et le préjudice subi. Pour cela il pourra tenter d'obtenir, avec l'accord des juges, les données de connexion du tiers auprès de son fournisseur d'accès à Internet, afin d'obtenir réparation sous forme de dommages et intérêts.

Section 3. Les atteintes à la tranquillité de l'internaute

80. Le droit à la tranquillité est associé à la notion de vie privée : c'est le droit de tout un chacun de ne pas subir d'atteinte dans le cadre de son intimité. Ce droit à la tranquillité, ou droit à être laissé tranquille, est né aux Etats-Unis sous le nom de *right to be left alone*.

L'étude du droit à être tranquille de l'internaute se fera en deux étapes : la première s'attachera aux sources de ce droit particulier, et la seconde énoncera les atteintes que peut subir la tranquillité de l'internaute et les moyens de défense dont dispose ce dernier.

§1. La construction du droit à la tranquillité

81. La construction du droit à être laissé tranquille s'est tout d'abord faite aux Etats-Unis. Aujourd'hui il commence à être consacré en France en ce qui concerne l'utilisation d'Internet[42]

A. Les origines du *right to be left alone*

82. Aux Etats-Unis, le *right to be left alone* fait partie intégrante du *right to privacy* depuis une décision *Holloman v. Life Ins. Co of Virginia* de la Cour suprême du sud de la Californie de 1940. En réalité le *right to be left alone* permet de protéger une partie de la vie privée des citoyens en empêchant que des tiers s'y immiscent par tout moyen. Pour autant les notions de vie privée et de tranquillité ne sont pas synonymes : il peut très bien y avoir une atteinte à la vie privée d'une personne sans que sa tranquillité ne soit touchée.

Aujourd'hui la notion de *right to be left alone* semble de plus en plus indépendante : en effet le fait de subir du *spamming* heurte le droit à la tranquillité de l'internaute et non sa vie privée. L'avènement des technologies de l'information et de la communication semble avoir fait prendre à la notion de tranquillité un sens tout autre dans le cadre des réseaux et télécommunications.

Lorsque l'internaute navigue sur Internet, le fait de disposer d'un droit à la tranquillité ne concerne plus seulement du droit de la protection de sa vie privée sur le réseau, mais d'un droit à naviguer sereinement sur la toile mondiale.

---

[42] Kassem, Hala. *L'internaute et son droit à être laissé tranquille.* Mémoire de DEA Informatique et Droit sous la direction du professeur Jean Frayssinet. Montpellier 2003

B. Le droit à être laissé tranquille en France

83. Le droit français ne contient pas de disposition relative à un droit à être tranquille. Toutefois la doctrine et la jurisprudence ont assimilé, de la même manière que la jurisprudence et la doctrine américaine, le droit à la tranquillité au droit à la vie privée de l'article 9 du code civil[43].

La construction en droit français serait donc la reprise de la construction américaine et on pourrait donc penser que les textes protecteurs de la vie privée des individus seraient également protecteurs de leur tranquillité.

Là encore, la réalité technologique n'est pas prise en compte : ce que l'on entend aujourd'hui par droit à la tranquillité de l'internaute est sensiblement différent, bien que proche, de son droit à la vie privée sur les réseaux. Ainsi l'atteinte à la vie privée de l'internaute pourra se faire par une atteinte à ses données de connexion en tant que données à caractère personnel. Néanmoins, il ne faut pas oublier que les textes protecteurs des données à caractère personnel, tels que la loi relative à l'informatique, aux fichiers et aux libertés du 6 janvier 1978 ou la directive mère relative à la protection des données à caractère personnel du 24 octobre 1995 et ses directives filles, sont avant tout protecteurs de la vie privée des personnes.

La Commission nationale de l'informatique et des libertés a toutefois reconnu indirectement un droit à la tranquillité des internautes dans son rapport « Publipostage électronique et la protection des données personnelles » en montrant que l'inconvénient majeur de la pratique du *spamming* est l'atteinte à la tranquillité de ces internautes.

La doctrine française semble plutôt accueillante à l'intégration d'un droit à la tranquillité autonome. Cette opinion se retrouve notamment dans les écrits de Jean Frayssinet[44], et de Michel Vivant et Christian Le Stanc[45]. Ces auteurs reconnaissent en effet aux internautes un véritable droit à être laissé tranquillité dans leur utilisation de l'Internet.

---

[43] Carbonnier, J. *Droit Civil.* Thémis

Lacabarats, A. *Vie privée et média*

[44] *Nouvelles technologies de l'information et de la communication et protection des libertés des consommateurs*. *Les libertés individuelles à l'épreuve des NTIC*, PUL, 2001, p 31 et s.

[45] *Lamy Droit de l'informatique et des réseaux*, éd. 2003

§2. Les actes portant atteinte à ce droit

84. Accorder un droit à une personne revient à lui offrir des moyens de protection contre des atteintes à ce droit. Concernant leur droit à la tranquillité, les atteintes susceptibles de frapper les internautes sont nombreuses. L'utilisation de l'Internet peut rapidement devenir fastidieuse du fait des *pop-up*, de la pratique du *spamming*, de l'indiscrétion des cookies et des *spywares*.

Les pop-up n'auront pas à être étudiés dans le cadre de l'accès de l'internaute aux données de connexion de tiers, car il existe des outils performant pour ne pas subir cette atteinte lorsque l'on navigue sur Internet. De plus, si le pop-up est clairement une atteinte à la tranquillité de l'internaute, il ne constitue pas une atteinte justifiant que l'internaute accède aux données de connexion de son émetteur dans le but d'une action en justice.

A. La pratique du *spamming*

85. La C.N.I.L. définit la pratique du *spamming* comme étant « l'envoi massif et répété de courriers électroniques non sollicités à des personnes avec lesquelles l'expéditeur n'a jamais eu de contact et dont il a capté l'adresse électronique de façon irrégulière »[46].

La C.N.I.L. pose ainsi des conditions pour qu'un message électronique soit considéré comme du *spam* : il faut que le message soit envoyé en nombre à une personne non connue dont l'adresse a été frauduleusement captée. Si la C.N.I.L. ne donne aucune précision du nombre de messages qui doivent être expédiés, elle donne deux critères de qualification d'un message en *spam* : la captation irrégulière de l'adressé du spammé et l'absence de relation personnelle avec lui.

La doctrine a aussi proposé sa définition du *spamming* : selon Michel Vivant et Christian Le Stanc *in* Lamy Droit de l'informatique et des réseaux, il s'agirait de l'envoi en nombre de courriers électroniques et le rapprochent des communications commerciales non sollicitées. C'est ici le fait que la communication ne soit pas sollicitée et qu'elle se fasse en nombre qui qualifie le *spam*.

[46] Voir le site Internet de la C.N.I.L. <*www.cnil.fr*>

Les organismes de lutte contre le *spamming*, que ce soit Caspam[47] ou encore Cypango[48], reprennent les critères d'envoi en nombre et de non-sollicitation de la part des internautes.

Le projet de loi pour la confiance en l'économie numérique envisage la pratique du *spamming* dans son article 12 et interdit « *la prospection directe, notamment la publicité, au moyen d'automates d'appel et de télécopieurs utilisant, sous quelque forme que ce soit, les coordonnées de toute personne qui n'a pas exprimé son consentement préalable à recevoir de tels appels* ». Bien que la loi n'use pas du terme de *spamming*, il n'en demeure pas moins que c'est bien cette pratique qui est visée.

Le droit communautaire a réagi face à l'atteinte au droit à être laissé tranquille des internautes avec la directive 2002/58/CE du 12 juillet 2002 qui entend protéger *« les abonnés contre toute violation de leur vie privée par des communications non sollicitées effectuées à des fins de prospection directe, en particulier au moyen d'automate d'appel, de télécopies et courriers électroniques, y compris les messages courts* ».

Lorsque l'internaute subira du *spamming*, il pourra demander au spammeur de stopper les envois. Si le spammeur continue de pratiquer le *spamming*, l'internaute pourra actionner les mécanismes connus de défense de ses données à caractère personnel, que le spammeur aura capté frauduleusement, ce qui permettra d'engager la responsabilité pénale de ce dernier. Certaines décisions de justice ont été jusqu'à décider de la résolution du contrat entre le spammeur et son fournisseur d'accès à Internet, comme par exemple le jugement du Tribunal de grande instance de Paris du 15 janvier 2002.

B. Le cas des cookies

86. Les cookies peuvent, comme nous l'avons vu, être constitutifs d'atteintes à la vie privée de l'internaute. De ce fait, les cookies empêchent également l'internaute d'utiliser Internet de manière tranquille. Il est possible pour l'internaute de désactiver l'acceptation des cookies dans son navigateur web mais de nombreux sites lui seront alors inaccessibles.

[47] <http://caspam.org/spam.html>

[48] <http://www.cypango.net/spam>

Dans le cas d'une atteinte à la vie privée de l'internaute, ce dernier pourra agir en responsabilité civile, voire pénale, contre le responsable du site Internet.

C. Les espiogiciels (ou *spywares* en anglais)

87. Le terme d'espiogiciel, qui provient de la contraction entre espion et logiciel, est un programme, ou une instruction contenu dans un programme, qui a pour but d'espionner les faits et gestes de l'internaute et d'en rendre compte à son concepteur ou à un tiers via le réseau Internet. Le logiciel peut également étudier tout ce qu'il y a sur le disque dur de l'internaute : ses fichiers, ses programmes…

Le logiciel espion pourra donc collecter des données de l'internaute à caractère personnel qui pourront être de natures diverses : liste des sites Internet visités, les cookies présents sur la machine, liste des documents de l'internaute, liste de ses programmes, liste de ses fichiers musicaux… Installer un logiciel de ce type sur la machine de l'internaute peut se faire pour plusieurs raisons : espionnage à des fins commerciales, atteintes directes envers l'internaute, vérification de la légalité du contenu de la machine… De grandes sociétés d'informatiques ont eu l'habitude d'installer des espiogiciels dans leurs programmes afin de savoir si les versions utilisées par les internautes étaient autorisées ou non.

Le problème est que les internautes n'ont la plupart du temps pas conscience qu'un mouchard rend compte à un tiers de leurs actes. L'intrusion d'un tel logiciel dans la machine de l'internaute est bien évidemment une atteinte à son droit à être laissé tranquille mais également à une atteinte à sa vie privée, à ses données à caractère personnel, et à l'intégrité de son système de traitement automatisé de données. L'internaute pourra donc agir au nom de toutes ces protections, comme nous l'avons montré précédemment.

De manière préventive, l'internaute peut également installer des protections techniques sur son ordinateur. Il pourra installer un pare-feu (firewall en anglais) qui est un « *dispositif informatique qui permet le passage sélectif des flux d'information entre un réseau interne et un réseau public, ainsi que la neutralisation des tentatives de pénétration en provenance du réseau public. Le terme pare-feu peut désigner plusieurs types de dispositifs de sécurité. Il peut s'agir d'un routeur (routeur filtrant), d'une station équipée de deux interfaces réseaux (bastion Internet), ou encore d'une combinaison de ces deux systèmes. Black Hole de Milkyway Networks, Guardian de*

NetGuard, et eNetwork d'IBM, sont des exemples de pare-feu. On peut également parler de coupe-feu »[49]. Il pourra également installer des logiciels qui détecteront les spywares lorsque ceux-ci tenteront d'envoyer des données à un tiers par le réseau tels que Little Snitch disponible sur le système d'opération Mac OS X.

[49] http://encyclopedie.journaldunet.com/definition/227/13/2/firewall/

Partie 3. L'accès aux données de connexion de l'internaute par des tiers

88. Plusieurs raisons peuvent pousser une personne à accéder aux données de connexion de l'internaute. Comme nous l'avons vu, l'internaute n'est pas sans défense face aux accès illégitimes dont ses données de connexion seraient les victimes. En effet, il peut combattre cet accès illicite en accédant lui-même aux données de connexion de la personne malveillante.

Toutefois, il est de nombreuses situations dans lesquelles des personnes peuvent légitimement avoir besoin d'accéder aux données de connexion d'un internaute, soit dans le respect des règles posées par la législation, française et communautaire, sur la protection des données à caractère personnel, soit par le besoin de la recherche de la justice.

Ces deux types d'accès permettent donc d'envisager d'une part un accès permis par le droit de la protection des données à caractère personnel (chapitre 1), et d'autre part un accès imposé pour les besoins de la justice (chapitre 2).

Chapitre 1. L'accès aux données de connexion de l'internaute permis par la législation sur les données personnelles

89. Le droit français et le droit communautaire ont mis en place un régime d'accès et de traitement des données à caractère personnel qui s'applique également aux traitements réalisés par Internet.

Ainsi, le responsable du traitement doit satisfaire à toute une série d'obligations.

En premier lieu, il doit remplir des formalités préalables à toute mise en place d'un traitement automatisé des données de connexion de l'internaute, avec des obligations envers la Commission nationale de l'informatique et des libertés et des obligations envers l'internaute dont les données de connexion sont traitées (section 1).

En second lieu, le responsable du traitement doit assurer certains principes relatifs à la qualité des données de connexion traitées (section 2).

Section 1. Les formalités préalables au traitement des données de connexion de l'internaute

90. Avant toute collecte et traitement de données à caractère personnel, les responsables de traitement doivent remplir une série d'obligations. Ces obligations sont très importantes au regard des principes généraux gouvernant la protection des personnes face aux traitements automatisés de données à caractère personnel. La première des obligations pour le responsable d'un traitement est de déclarer son traitement à la Commission nationale de l'informatique et des libertés soit par une simple déclaration soit par une demande d'autorisation. Ensuite, lorsqu'il aura déclaré ou reçu l'autorisation, le responsable de traitement devra informer les personnes de la réalisation d'un traitement automatisé de leurs données à caractère personnel et parfois en obtenir le consentement. Ceci nous permettra de distinguer entre les formalités préalables à remplir à l'égard de la C.N.I.L. et celles qui sont à remplir à l'égard des personnes concernées par le traitement.

§1. Les obligations du responsable du traitement envers la Commission nationale de l'informatique et des libertés

91. Cette obligation découle du Chapitre III de la loi n° 78-17 du 6 janvier 1978 intitulé « Formalités préalables à la mise en œuvre des traitements automatisés ». Le premier article de ce chapitre, l'article 14, explique qu'une des fonctions de la Commission nationale de l'informatique et des libertés est de veiller à ce que les traitements automatisés, publics ou privés d'informations nominatives, soient effectués conformément aux dispositions de la loi de 1978. C'est ce rôle de la C.N.I.L. qui impose aux responsables de traitement d'informations nominatives de remplir des formalités préalables à tout traitement. De ce fait, les responsables de traitement sont soumis à des procédures préalables à tout traitement automatisé d'informations nominatives. Cependant le projet de loi de transposition de la directive 95/46/CE du 24 octobre 1995 semble apporter des modifications dans ces procédures…

Le respect de ces formalités est très important. Le non-respect, y compris par négligence, des formalités préalables à la mise en œuvre des traitements est une infraction pénale prévue par

l'article 226-16 du code pénal qui prévoit une peine d'emprisonnement de trois années et une amende de 45 000 euros.

A. La procédure préalable à tout traitement sous la loi du 6 janvier 1978

92. Les formalités préalables sont de deux sortes, suivant la nature de la personne qui fait le traitement : la loi exige une autorisation de la C.N.I.L. lorsque le responsable du traitement est une personne publique, et elle exige une simple déclaration à la Commission lorsqu'il s'agit d'une personne privée.

1). Le régime d'autorisation

93. Le régime d'autorisation est prévu par l'article 15 de la loi qui dispose :

« *Hormis les cas où ils doivent être autorisés par la loi les traitements automatisés d'informations nominatives opérés pour le compte de l'Etat, d'un établissement public ou d'une collectivité territoriale, ou d'une personne morale de droit privé gérant un service public, sont décidés par un acte réglementaire pris après avis motivé de la Commission nationale de l'informatique et des libertés.*

Si l'avis de la Commission est défavorable, il ne peut être passé outre que par un décret pris sur avis conforme du Conseil d'Etat ou s'agissant d'une collectivité territoriale, en vertu d'une décision de son organe délibérant apprécié par décret pris sur avis conforme du Conseil d'Etat.

Si au terme d'un délai de deux mois renouvelable une seule fois sur décision du président, l'avis de la commission n'est pas notifié, il est réputé favorable ».

On pourrait penser que ce régime d'autorisation ne s'adresse pas aux acteurs de l'Internet, or ce serait une vision faussée de la situation. En effet, en pratique, il arrive fréquemment que le responsable d'un traitement automatisé de données à caractère personnel soit une personne relevant du droit public. Pour exemple, nous pouvons citer les sites Internet fournissant un service public tels que ceux des régies de transport, ou encore les sites des ministères… Les responsables de ces sites devront demander l'autorisation à la C.N.I.L. de faire un traitement d'informations nominatives pour les informations contenues dans le site ou pour les données à

caractère personnel des internautes collectées au moyen de cookies. En outre, il n'est pas impossible qu'un fournisseur d'accès à Internet soit une personne relevant du droit public…

Le responsable de traitement relevant du secteur public devra donc demander l'avis de la Commission qui aura un délai de réponse de deux mois renouvelable une fois.

Selon l'article 19 de la loi, la demande d'avis doit préciser certains éléments : la personne qui présente la demande, les caractéristiques, la finalité et la dénomination du traitement, mais aussi le service chargé de mettre en œuvre le traitement ainsi que le service auprès duquel s'exerce le droit d'accès et les catégories de personnes qui ont directement accès aux informations enregistrées. La demande devra également préciser quelles informations nominatives seront traitées, leur origine et leur durée de conservation, les dispositions prises pour assurer la sécurité des données, les rapprochements, interconnexions et mises en relation de ces informations. Enfin la demande devra préciser si le traitement est destiné à l'exportation des informations nominatives à l'étranger.

Si la réponse est favorable, l'autorisation sera faite par la publication d'un acte réglementaire ou un arrêté portant création du traitement. Le défaut de réponse de la C.N.I.L. vaut autorisation de réalisation du traitement.

2). Le régime de déclaration

94. Le régime de déclaration concerne les personnes du secteur privé. Ce principe est posé par l'article 16 de la loi de 1978 qui dit que « *les traitements automatisés d'informations nominatives effectués pour le compte de personnes autres que celles qui sont soumises aux dispositions de l'article 15 doivent préalablement à leur mise en œuvre, faire l'objet d'une déclaration auprès de la Commission Nationale de l'Informatique et des Libertés.*

Cette déclaration comporte l'engagement que le traitement satisfait aux exigences de la loi.

Dès qu'il a reçu le récépissé délivré sans délai par la Commission, le demandeur peut mettre en œuvre le traitement. Il n'est exonéré d'aucune de ses responsabilités ».

Cette situation s'appliquera dans la majorité des espèces : le plus souvent les fournisseurs d'accès sont des sociétés commerciales relevant du droit privé. Concernant la gestion de sites Internet, le cas est analogue : les sites commerciaux appartiennent à des sociétés commerciales et les autres

sites seront sous la responsabilité de personnes physiques… Le fournisseur d'accès ou d'hébergement, la société qui a son site de commerce électronique, ou le particulier qui a son site personnel, tous seront soumis à cette formalité de déclaration préalable à tout traitement lorsqu'ils feront des traitements automatisés de données personnelles.

La déclaration établie par les personnes relevant du secteur privé devra comporter les mêmes éléments que le demande d'avis des personnes relevant du droit public, en vertu du même article 19 de la loi de 1978. Cette déclaration est à faire à la C.N.I.L. Lorsque le traitement sera déclaré, la Commission rendra un récépissé qui contient le numéro d'enregistrement de la demande. Le récépissé atteste de la bonne réalisation des formalités par le demandeur et est synonyme d'autorisation de mise en œuvre du traitement.

Il est à noter qu'il existe un bordereau spécifique pour les déclarations des sites Internet disponible sur le site Internet de la C.N.I.L.[50].

3). Le recours aux normes simplifiées

95. « Pour les catégories les plus courantes de traitement à caractère public ou privé, qui ne comportent manifestement pas d'atteinte à la vie privée ou aux libertés, la Commission nationale de l'informatique et des libertés établit des normes simplifiées des caractéristiques mentionnées à l'article 19.

Pour les traitements répondant à ces normes, seule une déclaration simplifiée de conformité à l'une des ces normes est déposée auprès de la commission. Sauf décision particulière de celle-ci, le récépissé de déclaration est délivré sans délai. Dès réception de ce récépissé, le demandeur peut mettre en œuvre le traitement. Il n'est exonéré d'aucune de ses responsabilités ».

L'article 17 de la loi du 6 janvier 1978 prévoit ces normes simplifiées pour certaines catégories de personnes comme les bibliothèques qui se réfèrent à la norme simplifiée n° 9 concernant les traitements automatisés d'informations nominatives relatives à la gestion des prêts de livres, supports audiovisuels et œuvres artistiques.

[50] *<http://www.cnil.fr>*

Ces normes simplifiées ne semblent pas s'appliquer aux cas de l'Internet. Il était toutefois important de les exposer dans l'éventualité où une norme simplifiée venait à être délibérée en ce domaine.

4). Les traitements exclus de toutes formalités

96. Les traitements exclus des formalités sont les traitements manuels, les traitements issus de la comptabilité générale et les registres des membres ou des correspondants des églises ou des groupements à caractère religieux, philosophique, politique ou syndical.

Si les deux premiers types de traitements ne posent aucun problème au regard des traitements effectués *on-line*, il en est d'une autre manière pour les traitements d'informations nominatives effectués par des groupements religieux, politiques, syndicaux ou philosophiques…

Nous pouvons imaginer qu'un groupement politique va disposer d'un site Internet afin d'en faire la promotion. Ce groupement offre à ses membres, et uniquement à ses membres, un accès personnalisé sous la forme d'un contrôle par login et mot de passe. Cette situation entrerait parfaitement dans le cadre de l'article 31 de la loi de 1978 : aucun contrôle ne pourrait être exercé à l'encontre de ce groupement.

B. Les modifications apportées par le projet de loi de transposition de la directive du 24 octobre 1995

97. Les modifications apportées par le projet de loi de transposition de la directive sont nombreuses notamment au regard des demandes d'avis et des déclarations. En effet, avec ce projet de loi de transposition, nous assisterons à l'abandon du critère organique consacré par la loi de 1978 et à l'émergence d'un nouveau critère basé sur la matérialité du traitement.

1). L'abandon du critère organique

98. Si la loi du 6 janvier 1978 faisait une distinction, selon un critère organique, entre les formalités à réaliser, le projet de loi de transposition de la directive de 1995 adopte une démarche radicalement différente. La dichotomie opérée par la loi de 1978 semblait résulter d'une dangerosité plus élevée des traitements réalisés par les personnes publiques au regard de la

protection de la vie privée et des libertés individuelles. Ceci peut se comprendre au regard du projet S.A.F.A.R.I. élaboré dans les années 1970. S.A.F.A.R.I. signifie système automatisé pour les fichiers administratifs et le répertoire des individus qui reposait, et c'était là sa principale caractéristique, sur l'utilisation systématique du NIR comme identifiant unique pour toutes les administrations. Or la presse eut connaissance de ce projet et titra « S.A.F.A.R.I. ou la chasse aux Français » et le projet sera abandonné en raison de l'impact médiatico-politique de cette annonce.

Il apparaît aujourd'hui réducteur de dire que les traitements réalisés par l'autorité publique sont plus dangereux que ceux opérés par les personnes privées. C'est pourquoi le projet de loi de transposition de la directive abandonne ce critère organique au profit d'un critère matériel.

2). L'émergence d'un critère matériel

99. Le critère matériel se manifeste de deux façons : la teneur des formalités dépendra essentiellement des données collectées ou en considération de la finalité des traitements réalisés.

a). Le régime de déclaration : le régime de principe

100. Le régime de déclaration des traitements automatisés de données à caractère personnel est le régime de droit commun.Ces traitements doivent faire l'objet d'une déclaration auprès de la C.N.I.L. en vertu de l'article 22 du projet de loi de transposition. L'article 23 exige que le demandeur déclare que le traitement satisfasse les exigences de la loi. La déclaration pourra se faire par voie électronique et la commission délivrera alors un récépissé, par voie postale ou électronique. A la réception du récépissé, le demandeur pourra mettre en œuvre le traitement.

Ce type de régime concernera a priori les acteurs du monde de l'Internet, qu'ils soient fournisseurs d'accès ou d'hébergement, société ou particulier responsable d'un site Internet. Dès lors qu'ils envisageront de traiter des données à caractère personnel, ils devront déclarer ce traitement préalablement à toute mise en œuvre.

Un régime de déclaration simplifiée sera également mis en place par l'établissement de normes par la C.N.I.L. Ce régime s'appliquera aux catégories les plus courantes de traitements automatisés de données à caractère personnel, dont la mise en œuvre ne sera pas susceptible de porter atteinte aux libertés individuelles et à la vie privée des personnes. Les normes élaborées

par la commission devront définir quelles seront les finalités des traitements, les données traitées, les personnes concernées, les destinataires qui se verront communiquer les données et la durée de conservation des données.

b). Les exceptions au régime de principe

101. Les exceptions au régime de déclaration préalable sont de deux ordres : soit les traitements seront exonérés de formalité, soit ils seront soumis à autorisation.

Certains traitements sont exonérés de toutes formalités par l'article 22.II du projet de loi de transposition de la directive. Ce sont les traitements dont la finalité est de tenir un registre public destiné à l'information du public et ouvert à la consultation de celui-ci. Sont également exonérés les traitements de données faits par tout organisme à but non lucratif, à caractère religieux, philosophique, politique ou syndical, concernant les membres de celui-ci. La C.N.I.L. pourra ajouter des catégories de traitements qui pourront bénéficier de cette exonération.

D'autres traitements seront soumis à autorisation. Ainsi lorsque les traitements porteront sur des données sensibles, génétiques, relatives aux infractions ou aux condamnations, contenant le numéro d'inscription au répertoire national d'identification des personnes physiques, ou encore biométriques, ils seront soumis à l'autorisation de la commission. Il en sera de même lorsque la finalité du traitement sera d'exclure du bénéfice d'un droit, d'une prestation ou d'un contrat ou l'interconnexion entre des fichiers de nature différente.

L'autorisation par arrêté du ou des ministres compétents concerne les traitements qui intéressent la sûreté de l'Etat, la défense ou la sécurité publique, ainsi que ceux qui ont pour objet la prévention, la recherche ou la poursuite des infractions pénales, ou encore l'exécution des condamnations pénales ou des mesures de sûreté sont concernés. Cet arrêté est pris après avis motivé et publié de la C.N.I.L.

L'autorisation par décret pris en Conseil d'Etat concerne les traitements mis en œuvre pour le compte de l'Etat, ou pour le compte des services de l'Etat et portant sur les données comportant le numéro d'inscription des personnes au répertoire national d'identification des personnes physiques, ou la totalité ou quasi-totalité de la population de la France.

§2. Les obligations du responsable du traitement envers les personnes concernées par ce traitement

102. Ces obligations sont assez proches : le responsable a l'obligation d'informer les personnes dont les données font l'objet d'un traitement. Parfois l'obligation pourra aller jusqu'à ce que le responsable ait pour obligation d'obtenir un consentement de la part de ces personnes.

A. L'obligation d'informer les personnes concernées

103. Le responsable d'un traitement automatisé de données à caractère personnel doit donner des informations aux personnes concernées par le traitement.

Les informations à donner sont de deux ordres suivant la relation qui existe entre le responsable du traitement et la personne concernée par ce traitement.

Soit il existe une relation directe entre le responsable du traitement et la personne concernée et s'applique alors l'article 27 de la loi du 6 janvier 1978 et l'article 10 de la directive du 24 octobre 1995. L'article 27 dispose que les informations à communiquer à la personne concernée sont le caractère obligatoire ou facultatif des réponses, les conséquences d'un défaut de réponse, les personnes physiques ou morales destinataires des données, et l'existence d'un droit d'accès et de rectification. L'article 10 de la directive reprend les mêmes éléments et y ajoute que le responsable du traitement doit exposer la finalité du traitement. Lorsque les données sont collectées au moyen d'un questionnaire la loi française prévoit qu'il doit être fait mention de ces prescriptions, sous peine d'une contravention de 5ème classe par questionnaire irrégulier.

Soit il y a cession des données collectées au profit d'une tierce personne : cette situation n'est pas prévue par la loi de 1978. L'article 11 de la directive de 1995 dispose que la personne dont les données la concernant sont traitées devra être informée de la cession des données au plus tard lors de la première communication et avoir connaissance des informations suivantes : l'identité du responsable du traitement, les finalités du traitement, les catégories de données concernées, les destinataires et l'existence du droit d'accès et de rectification. En pratique, c'est souvent celui qui fait l'acquisition des données qui devra informer la personne concernée. Cette obligation permet une certaine traçabilité des données et le respect des droits des individus.

Le projet de loi de transposition de la directive de 1995 reprend ces dispositions et en ajoute à l'égard des fournisseurs de service de télécommunication en ligne. Ces derniers seront exonérés

de l'obligation d'information en vertu de l'article 32-I bis qui énonce que les dispositions relatives à l'obligation d'information ne sont pas applicables « *aux informations stockées dans l'équipement terminal de l'utilisateur ou l'inscription d'informations dans l'équipement terminal de l'utilisateur :*

- *soit a pour finalité exclusive de permettre ou faciliter la communication par voie électronique ;*
- *soit est strictement nécessaire à la fourniture d'un service de communication en ligne à la demande expresse de l'utilisateur* ».

Les fournisseurs d'accès à Internet et d'hébergement n'auraient aucune obligation d'information si le projet de loi était adopté en l'état. En revanche les responsables de site Internet devront fournir aux personnes concernées les informations requises par l'article 32-I. L'article dispose que « *toute personne utilisatrice des réseaux de communication électroniques doit être informée de manière claire et complète par le responsable du traitement ou son représentant :*

- *de la finalité de toute action tendant à accéder, par voie de transmission électronique, à des informations stockées dans son équipement terminal de connexion, ou à inscrire, par la même voie, des informations dans son équipement terminal de connexion ;*
- *des moyens dont elle dispose pour s'y opposer* ».

Cette disposition s'applique particulièrement aux cookies puisqu'ils sont inscrits par voie de transmission électronique dans l'ordinateur de l'internaute et que le site y accède par la même voie. Les responsables de site Internet sont donc particulièrement visés par les dispositions du projet de loi de transposition de la directive de 1995.

B. L'obligation d'obtenir le consentement des personnes concernées

104. L'obtention du consentement de la personne concernée n'est pas une obligation au sens de la loi du 6 janvier 1978. Cette exigence est prévue par l'article 7 de la directive de 1995 qui dispose que « *le traitement de données à caractère personnel ne peut être effectué que si la personne a indubitablement donné son consentement* ». Mais l'article pose une série d'exceptions : ainsi le consentement ne sera notamment pas requis lorsque le traitement sera nécessaire à la réalisation de l'intérêt légitime poursuivi par le responsable. L'intérêt légitime

poursuivi par le responsable du traitement ne doit pas porter préjudice à l'intérêt et les droits et libertés fondamentaux de la personne concernée par le traitement. En pratique, le responsable du traitement aura toujours un intérêt légitime à effectuer le traitement et il apparaîtra que le consentement de la part de la personne concernée ne sera que très peu exigé.

Dans le cadre de leur activité, les fournisseurs d'accès à Internet et d'hébergement ont véritablement un intérêt légitime à collecter et à traiter les données à caractère personnel de leurs utilisateurs, données qui se manifesteront également par des données de connexion. En effet, le fournisseur d'accès à Internet a réellement besoin des données de connexion des internautes afin de fournir la connexion et afin d'assurer la facturation de ses clients. Pour le fournisseur d'hébergement, l'intérêt légitime est également présent car il est techniquement contraint de traiter les données de connexion afin d'offrir un hébergement à ses clients.

C'est encore dans le cadre de l'activité des sites Internet qu'il sera plus contestable de dire qu'il y a un intérêt légitime. Pour les sites commerciaux, l'intérêt légitime sera présent lorsque le site gérera l'accès des clients aux espaces de paiements par un système de nom d'utilisateur et de mot de passe. En revanche, concernant le site d'un particulier, l'intérêt légitime sera plus difficile à démontrer et il y aura, dans la plupart des espèces, obligation pour le responsable du traitement des cookies d'obtenir le consentement des personnes concernées préalablement à ce traitement.

Le projet de transposition de la directive reprend ce principe d'obtention du consentement de la personne concernée dans son article 7.

Section 2. Les principes relatifs à la qualité des données traitées

105. Ces principes sont énoncés par les textes nationaux et communautaires, et donnent à la personne dont les données à caractère personnel sont visées par un traitement des garanties sur le comportement des responsables de traitement. Ces principes sont celui de collecte loyale et licite des données, celui de respecter la finalité du traitement, celui de garantir la sécurité des données et enfin celui de conserver les données de manière raisonnable.

§1. Le principe de loyauté et de licéité

106. La loi du 6 janvier 1978 interdit à toute personne de procéder à une collecte de données à caractère personnel par moyen frauduleux, déloyal ou illicite. Ce principe est posé par l'article 25 de la loi.

Une collecte par moyen illicite sera facile à démontrer car ce sera une collecte effectuée en contradiction avec les textes normatifs, comme, par exemple, la violation de l'obligation d'information à la C.N.I.L.

En revanche, un moyen déloyal de collecte semble être plus délicat à prouver. En effet, la loyauté est moins une façon de se comporter qu'une notion juridique, on pourrait l'assimiler au comportement du « bon père de famille ». L'appréciation du caractère loyal de la collecte se fera donc en pratique au cas par cas par rapport à une norme de référence. Dans le cadre du traitement de données à caractère personnel, le fait de collecter loyalement ces données signifie que la personne dont les informations nominatives sont sollicitées devra avoir été prévenue qu'une telle collecte est effectuée. La personne visée par la collecte ne doit pas être trompée et doit avoir connaissance que des données la concernant vont être collectées et traitées. Le principe de collecte loyale et licite se traduit par un certain nombre d'obligations à la charge du responsable de traitement. Le responsable d'un traitement de données de connexion devra informer préalablement les internautes dont les données sont recueillies, et devra parfois en obtenir l'accord exprès concernant les données sensibles. Mais ce principe induit également que le responsable, qu'il soit fournisseur de service ou webmestre, s'interdit d'enregistrer des données comme les condamnations pénales ou encore d'utiliser d'autres fichiers constitués à d'autres fins

comme source d'information. Notons que dans l'exercice de leurs activités, les acteurs de l'Internet auront rarement accès aux condamnations pénales des internautes. Cette situation semble impossible en pratique.

En pratique, les comportements déloyaux sont très nombreux. Ces comportements sont rarement ceux adoptés par les prestataires de fourniture d'accès à Internet ou d'hébergement mais plutôt ceux des responsables de sites Internet. Les cookies des sites Internet seront loyaux si la personne concernée est prévenue de leur existence. Si l'internaute n'a eu d'information sur la présence de cookies de la part du webmestre, alors on pourrait considérer que la collecte effectuée par ce dernier se fera par moyen déloyal.

La collecte sera dans tous les cas considérée comme déloyale lorsqu'elle sera réalisée malgré l'opposition de l'internaute. Le code pénal prévoit cette éventualité dans son article 226-18 et punit d'une peine de cinq années d'emprisonnement et de 300 000 euros d'amende le fait de collecter des données à caractère personnel par tout moyen frauduleux, déloyal ou illicite, mais aussi le fait de traiter les informations nominatives d'une personne lorsque celle-ci a exercé son droit d'opposition, fondé sur des raisons légitimes.

Nous voyons donc que les peines encourues sont loin d'être anodines, que ce soit pour une collecte déloyale ou pour un traitement malgré opposition. Cependant, bien que les atteintes soient nombreuses en pratique, il y a très peu de litiges concernant ces actes.

La directive du 24 octobre 1995 contient le principe de loyauté et de licéité des collectes dans son article 6-1 a) qui énonce « *Les Etats membres prévoient que les données à caractère personnel doivent être traitées loyalement et licitement* ». Le projet de loi de transposition de cette directive reprend cette même structure dans son article 6-1 : « *Un traitement ne peut porter que sur des données qui satisfont aux conditions suivantes, qu'il incombe au responsable du traitement de faire respecter : les données sont collectées et traitées de manière loyale et licite* ». Dans le projet, la loyauté et la licéité ne touchent pas seulement la collecte mais également le traitement des données à caractère personnel. Cela signifie que le responsable du traitement aura une obligation continue de loyauté à l'égard de la personne concernée par les informations.

§2. Le principe de finalité

107. Le respect de la finalité prévue pour le traitement est une obligation qui découle de l'article 19 de la loi du 6 janvier 1978 qui énonce les éléments que la demande d'avis ou la déclaration doivent comprendre. En effet, ces demandes doivent préciser la finalité du traitement. La directive de 1995, ainsi que le projet de loi de transposition la concernant, contient également ce principe de finalité.[51] Le traitement d'informations nominatives est créé pour atteindre un objectif auquel doit correspondre son contenu. La finalité du traitement n'est pas accessoire, car le responsable sera lié à cet objectif dans la réalisation de son traitement de données à caractère personnel. La détermination de la finalité du traitement devra donc être précisément et clairement exposée par la personne qui se chargera d'effectuer les formalités préalables auprès de la Commission nationale de l'informatique et des libertés.

Concernant le fournisseur d'accès et le fournisseur d'hébergement, ils n'auront pas une grande marge de manœuvre dans la détermination de la finalité de leurs traitements. Le fournisseur d'accès et le fournisseur d'hébergement traitent des données de connexion d'internautes, afin de gérer les accès aux services pourvus. Sans traitement des données de connexion des internautes, il serait impossible pour le fournisseur d'accès à Internet de leur permettre de se connecter au réseau. De même, l'hébergeur serait dans l'incapacité de définir quel internaute dispose de quel espace sur ses serveurs s'il ne traite pas les données de connexion de ces derniers. Dans la mesure où ces prestataires de service sont des intermédiaires techniques et de facturation, la finalité de leur traitement sera aisée à mettre à jour. Néanmoins, si ces prestataires utilisent les données de connexion à d'autres desseins que ceux de la finalité de leur traitement, on pourra considérer qu'ils auront commis un détournement de finalité.

Concernant le responsable d'un site Internet, les finalités pouvant être exposées dans le cadre des formalités préalables auprès de la C.N.I.L. peuvent être multiples. Un site commercial aura par exemple besoin de traiter des données de connexions dans le but d'offrir aux internautes clients un espace de commande de produits et de paiement en ligne. Un site communautaire devra collecter des données afin de permettre aux internautes membres de cette communauté un accès individuel aux différentes sections du site. Là encore, les responsables ne peuvent se détourner de

[51] Article 6-1 b) de la directive 95/46/CE du 24 octobre 1995

la finalité qu'ils auront défini dans les formalités préalables. Pourtant ces responsables pourront être facilement tentés de détourner la finalité de leur traitement afin de cibler les internautes venant sur leurs sites…

Les sanctions auxquelles s'exposent des personnes ayant commis un détournement de finalité sont pourtant assez lourdes : l'article 226-21 du code pénal punit « *le fait, par toute personne détentrice d'informations nominatives à l'occasion de leur enregistrement, de leur classement, de leur transmission ou de toute autre forme de traitement, de détourner ces informations de leur finalité telle que définie par la disposition législative ou l'acte réglementaire autorisant le traitement automatisé, « ou par la décision de la Commission nationale de l'informatique et des libertés autorisant un traitement automatisé ayant pour fin la recherche dans le domaine de la santé, » ou par les déclarations préalables à la mise en œuvre de ce traitement* » par une peine de cinq ans d'emprisonnement et de 300 000 euros d'amende.

L'article 6 de la directive communautaire de 1995 pose également des principes relatifs à la qualité des données au regard de la finalité du traitement. Selon cette disposition, les données à caractère personnel doivent être « *adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et pour lesquelles elles sont traitées ultérieurement* ». Ce principe signifie que les responsables de traitement ne doivent traiter que les données nécessaires à la réalisation de la finalité du traitement. Ainsi un fournisseur d'accès à Internet ou d'hébergement devra collecter et traiter certaines données de connexion concernant l'internaute comme son adresse IP ou son login, mais en aucun cas il ne devra traiter la profession ou l'âge de l'internaute dans le cadre de la fourniture technique du service.

En vertu de la directive, les données doivent être « *exactes et, si nécessaire, mises à jour ; toutes les mesures raisonnables doivent être prises pour que les données inexactes ou incomplètes, au regard des finalités pour lesquelles elles sont collectées ou pour lesquelles elles sont traitées ultérieurement, soient effacées ou rectifiées* ». La directive fait reposer sur les épaules du responsable du traitement une obligation de rectification des données. Le fournisseur d'accès à Internet devra donc veiller à ce que le login de l'internaute soit exact (si l'internaute a la possibilité de changer de login) et il devra collecter les dates et heures exactes de connexion et de déconnexion et non pas seulement la date de connexion…

§3. Le principe de sécurité

108. L'obligation de sécurité qui pèse sur le responsable d'un traitement automatisé de données à caractère personnel est conséquente. L'article 29 de la loi du 6 janvier 1978 dit 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* ».

Les données de connexion des internautes peuvent susciter la convoitise de nombreuses personnes tant ces données permettent une identification précise, bien qu'indirecte, des personnes auxquelles elles se rapportent. Certaines personnes peuvent vouloir accéder aux données de connexion détenues par les fournisseurs d'accès à Internet afin d'usurper l'identité des internautes et commettre des infractions par le biais d'Internet. Ces personnes pourraient ainsi vouloir accéder à certains systèmes de traitements automatisés de données telles que les institutions bancaires ou encore les réseaux de la défense nationale en utilisant l'identité d'honnêtes internautes sur lesquels la faute retombera. D'autres personnes voudront accéder aux cookies posés par un site sur le système de l'internaute afin une fois encore d'en usurper l'identité et de commander des produits en ligne. En effet, certains sites marchands conservent les coordonnées bancaires de leurs clients dans les cookies, ainsi lorsque le client se connecte, il a juste besoin de désigner les produits afin de les commander. Il sera alors aisé pour une personne malveillante de se faire livrer des produits à forte valeur à une autre adresse que celle de la personne usurpée.

La directive du 24 octobre 1995 accorde également une grande importance à l'obligation de sécurité à l'article 17 qui oblige le responsable du traitement à mettre en œuvre « *les mesures techniques et d'organisation appropriées pour protéger les données à caractère personnel contre la destruction accidentelle ou illicite, la perte accidentelle, l'altération, la diffusion ou l'accès non autorisés, notamment lorsque le traitement comporte des transmissions de données dans un réseau, ainsi que contre toute autre forme de traitement illicite. Ces mesures doivent assurer, compte tenu de l'état de l'art et des coûts liés à leur mise en œuvre, un niveau de sécurité approprié au regard des risques présentés par le traitement et de la nature des données à protéger* ». Lorsqu'une atteinte aux données de connexion de l'internaute sera survenue, le responsable du traitement qui n'aura pas rempli cette obligation, ce dernier sera sanctionné par

une peine de cinq ans d'emprisonnement et d'une amende de 300 000 euros en vertu de l'article 226-17 du code pénal. Cet article dispose qu'est puni « *le fait de procéder ou de faire procéder à un traitement automatisé d'informations nominatives sans prendre toutes les précautions utiles pour préserver la sécurité de ces informations* ».

§4. Le principe de conservation des données pendant un délai raisonnable

109. La durée de conservation des données de connexion de l'internaute est elle aussi régie par la législation sur la protection des données à caractère personnel et notamment la loi du 6 janvier 1978, en son article 28. Ainsi, les données de connexion de l'internaute ne pourront être conservées sous forme nominative plus longuement que la durée nécessaire à la finalité pour laquelle elles ont été collectées ou traitées, sauf exceptions. Ces exceptions concernent les buts statistiques, historiques ou scientifiques. La durée de conservation des données de connexion est tributaire des finalités du traitement lorsqu'elle n'est pas donnée dans la demande d'avis ou dans la déclaration auprès de la C.N.I.L. La directive relative à la protection des données à caractère personnel de 1995 reprend cette règle dans son article 6-1 e).

Les fournisseurs d'accès à Internet, les hébergeurs et les responsables de sites Internet devront donc fixer une durée raisonnable de conservation des données sous forme nominative, par rapport à la finalité recherchée.

Si l'opérateur conserve les données au-delà de la période énoncée dans la déclaration ou par rapport à la réalisation de la finalité du traitement, il risque selon l'article 226-20 une peine de trois années d'emprisonnement et une amende de 45 000 euros.

Cependant dans certaines situations, des lois spécifiques enjoignent les responsables de traitement à conserver les données de connexion des internautes pendant une durée plus longue que celle de la réalisation de la finalité du traitement ou que celle énoncée dans la demande d'avis ou dans la déclaration préalable. Le plus souvent, ces lois sont protectrices de l'ordre public et visent à faire cesser certains types d'infractions.

Chapitre 2. L'accès aux données de connexion de l'internaute requis par des motifs d'ordre judiciaire

110. Il s'agirait ici d'un abus de langage de parler d'un accès aux données de connexion de l'internaute par l'autorité judiciaire. En réalité, les autorités compétentes ne prendront connaissance de ces informations qu'indirectement. Ce n'est donc pas un accès « direct » qu'aura l'autorité judiciaire sur les données de connexion des internautes, en ce sens que ce n'est pas elle qui, techniquement, accèdera aux données. L'autorité judiciaire sera en effet contrainte de se tourner vers les prestataires techniques que sont les fournisseurs d'accès à Internet et le fournisseur d'hébergement de contenu.

Cet accès indirect de la justice aux données de connexion se fera donc en deux temps : tout d'abord, en imposant aux prestataires techniques de conserver les données de connexion de leurs usagers pendant un certain temps. Dans la mesure où ces prestataires ont la possibilité de conserver les données de connexion de leurs internautes à des fins de facturation, il était intéressant de garder ces éléments d'identification à des fins, envisageables, de justice. Ensuite, il pourra être imposer aux prestataires techniques une obligation de divulgation des données de connexion de l'internaute, à des fins probatoires.

Cependant, il sera possible d'envisager que la justice veuille constater des infractions en flagrant délit sur Internet : il pourrait s'agir par exemple de surveiller une personne sur un réseau de peer-to-peer. Les autorités de police pourraient alors conserver l'adresse IP de l'internaute qui envoie des fichiers musicaux afin de le poursuivre ultérieurement en contrefaçon. En pratique, peu d'affaires font état de ce genre de manipulations en France.

Section 1. Une obligation de conservation des données de connexion de l'internaute

111. Les prestataires techniques sont de plus en plus sollicités par le législateur pour conserver les données de connexion des internautes. Si cette obligation nécessite des coûts de stockage et de gestion importants, il n'en demeure pas moins que c'est un mal nécessaire à la constatation des infractions en ligne. Cette obligation de conservation peut avoir en pratique deux fondements principaux en raison des infractions qu'il est possible de commettre sur Internet : le fondement des infractions de cyber-criminalité et le fondement des délits de presse.

§1. Une obligation de conservation fondée sur la lutte contre la cyber-criminalité

112. Le fournisseur d'accès à Internet est assurément la personne la mieux placée pour constater si des infractions dites de cyber-criminalité sont commises par ses usagers. Comme nous l'avons vu les infractions de cyber-criminel concernent les atteintes aux systèmes de traitement automatisé de données réprimées aux articles 323-1 et suivants du code pénal, mais on peut également considérer que d'autres infractions pourront entrer dans cette catégorie comme par exemple les actes de téléchargements illégaux de fichiers musicaux sur les réseaux peer-to-peer. Ces téléchargements sont considérés comme de véritables contrefaçons par certains[52] (notamment les industriels du disque) et leurs auteurs peuvent donc être assimilés à des cyber-criminels.

Lors de procédures judiciaires, les fournisseurs d'accès seront en première ligne : les juges n'hésiteront pas à leur demander de leur fournir les données de connexion des internautes ayant commis des actes cyber-criminels. Cependant quelles données seront requises par l'autorité judiciaire ?

[52] Pour un avis divergent, voir les dernières interventions de Jean Vincent, de l'ADAMI qui considère le téléchargement de fichiers musicaux par peer-to-peer comme une véritable application du droit à la copie privée, sous réserve de l'existence d'une licence légale.

La directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002, concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques, définit les données concernées. Son article 2b) définit les données relatives au trafic comme étant « *toutes données traitées en vue de l'acheminement d'une communication par un réseau de communications électroniques ou de sa facturation* ». Concernant ces données, la directive estime qu'elles doivent être rendues anonymes ou effacées lorsqu'elles ne sont plus nécessaires à la transmission d'une communication. Cependant les fournisseurs d'accès pourront conserver ses données à des fins de facturation. Les données relatives au trafic sont les données de connexion des internautes : elles comprennent des éléments d'identification des usagers (adresse IP, login) et le moment où ceux-ci ont été connectés.

La loi n° 2001-1062 du 15 novembre 2001, relative à la sécurité quotidienne, porte modification du code des postes et des télécommunications en son article 29. Ainsi le code des postes exige aujourd'hui que, pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales, et dans le seul but de permettre la mise à disposition de l'autorité judiciaire d'informations, la durée maximale de conservation des données peut être repoussée d'un an, avant effacement ou anonymisation (article L 32-3-1 II du code des postes et des télécommunications). Le paragraphe IV de l'article L 32-3-1 prévoit que les données faisant l'objet de cette mesure sont les données portant exclusivement sur l'identification des personnes utilisatrices des services fournis par les opérateurs et sur les caractéristiques techniques des communications assurés par ceux-ci. Ces données ne peuvent porter sur le contenu des correspondances échangées ou des informations consultées. C'est donc bien les données de connexion de l'internaute que les opérateurs devront conserver à des fins judiciaires, même si un décret en Conseil d'Etat doit être pris afin d'énumérer les données à garder.

Les données de connexion des internautes pourront donc ici servir de moyens de preuve au bénéfice de l'autorité judiciaire qui voudra démontrer que les internautes visés sont bien des cyber-criminels.

Concernant la durée de conservation de ces données, le débat a été âpre : les prestataires et les diverses associations telles que l'association des fournisseurs d'accès voulaient une durée de conservation des données de connexion dans le cadre de fins judiciaires alignée sur la durée

permise à des fins de facturation, c'est-à-dire trois mois[53]. La Commission nationale de l'informatique et des libertés s'est présentée elle-même comme favorable à une telle durée de conservation. Pour sa part, le groupe de travail de l'article 29 a estimé dans une recommandation de 1999, relative à la préservation des données de trafic par les fournisseurs de services Internet pour le respect du droit, que le moyen le plus efficace de réduire « *les 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 télécommunication et de services internes 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 de l'article 29 a réaffirmé ce principe en 2003. En d'autres termes, que la durée de conservation pour des fins judiciaires ne dépassent pas trois mois. Mais les législateurs de la loi relative à la sécurité quotidienne mentionnée ci-dessus ont eu une autre vision et ont adopté une durée de conservation des données de connexion par les prestataires techniques d'une année.

§2. Une obligation de conservation fondée sur la lutte contre les infractions de presse

113. Certaines infractions de droit commun, et qui tendraient à engager la responsabilité civile de leur auteur, peuvent se retrouver dans le giron du droit pénal, et notamment du droit pénal spécial de la presse. C'est le cas pour la diffamation et pour l'injure notamment. Aux côtés de ces infractions se situent d'autres infractions réprimées par la loi du 29 juillet 1881 : la provocation et l'apologie de crimes et délits, les délits contre la chose publique, certaines publications interdites, ou encore la contestation de crime contre l'Humanité. Le risque est grand sur Internet de voir des sites proposer ce type de contenu. Certaines affaires récentes l'ont montré, comme, par exemple, lorsqu'il y a eu une tentative d'attentat contre le Président de la République française, Jacques Chirac. Les sites radicaux et extrémistes se multiplient sur la toile mondiale et il apparaît nécessaire de réprimer ce type d'atteinte. De même, les atteintes aux personnes par la

[53] Voir le Forum des droits de l'Internet, 5 novembre 2001

diffamation[54] ou par l'injure[55] seront fréquentes sur les sites web : il n'est en effet pas peu fréquent que des internautes aient des comportements peu révérencieux, sous couvert d'une liberté d'expression en ligne qu'ils estiment sans borne.

Le droit de la presse est un droit particulier qui joue sur un régime de responsabilité éditoriale dite « en cascade » : ainsi cette responsabilité pèse en premier lieu sur le directeur de publication, puis à défaut sur l'auteur… Pour que le droit de la presse s'applique, il faut qu'il y ait une communication au public avec exigence d'une fixation préalable. Si l'on suit cette définition, la communication sur Internet est indubitablement soumise au droit de la presse. Cependant il peut apparaître difficile de déterminer qui est le directeur de publication d'un site Internet. C'est pourquoi le législateur est intervenu afin de clarifier la situation et impose certaines obligations aux fournisseurs d'hébergement : celui-ci doit conserver les données de connexion des internautes qui fournissent du contenu en ligne.

La loi sur la confiance en l'économie numérique du 21 juin 2004 reprend le principe de la loi de 1986 sur la liberté de communication en énonçant que la communication au public par voie électronique est libre. Pour les éditeurs de contenu en ligne, la loi prévoit dans son article 6-III que l'éditeur d'un site Internet doit mettre à la disposition du public plusieurs informations, notamment des éléments d'identification. Les personnes n'agissant pas à titre professionnel devront donc indiquer les coordonnées de leur hébergeur[56], qui disposera des éléments d'identification de la personne. Dans ce cas précis, les juges n'auront *a priori* pas à connaître des données de connexion des internautes afin de lancer leurs poursuites et investigations car en saisissant l'hébergeur ils pourront connaître le responsable du site. Toutefois le recours aux données de connexion reste possible dans la mesure où le fournisseur d'hébergement peut savoir si le contenu a bien été mis en ligne par l'internaute qui bénéficie de l'espace.

En effet, concernant les prestataires techniques, ceux-ci doivent conserver les « *données de nature à permettre l'identification de quiconque a contribué à la création du contenu ou de l'un*

[54] La loi sur les délits de presse définit la diffamation comme « *toute allégation ou imputation d'un fait qui porte atteinte à l'honneur ou à la considération de la personne ou du corps auquel le fait est imputé* »

[55] La loi sur les délits de presse définit l'injure comme « *toute expression outrageante, terme de mépris ou invective qui ne renferme l'imputation d'aucun fait* »

[56] La loi du 21 juin 2004 définit l'hébergeur comme la personne qui assure « *le stockage des signaux, d'écrits, d'images, de sons ou de messages de toute nature fournis par les destinataires de ces services* ».

des contenus ». Les données à conserver doivent faire l'objet d'un décret, qui n'a pas été pris depuis 2000 et l'introduction de cette disposition dans la loi de 1986. Il y a fort à parier qu'il s'agira des données permettant l'identification des personnes, donc des données de connexion des internautes.

La durée de conservation de ces données est difficile à déterminer. Il semble que la durée à prendre en compte est celle de une année. Cette solution est logique dans la mesure où la prescription des délits de presse est d'une durée de trois mois ou d'un an selon les infractions, à compter du jour de la publication du message litigieux. Il y a donc un alignement parfait entre le point de départ du délai de prescription des infractions de presse et le point de départ du délai de conservation des données de connexion de l'internaute. La fin du délai de prescription (maximal) coïncidera donc avec la fin du délai de conservation des données de connexion de l'internaute par le prestataire technique.

Section 2. Une obligation de divulgation des données de connexion de l'internaute

114. L'obligation de divulguer les données de connexion des internautes est le corollaire logique de l'obligation de conserver ces données. Sans divulgation, la conservation n'aurait que peu d'intérêt.

Si l'obligation de divulguer les données de connexion des internautes est imposée dans de nombreux textes récents, il n'en demeure pas moins qu'il s'agit d'une obligation ancienne et générale, déjà consacrée par le code civil et les règles de procédure.

§1. Une obligation d'apporter son concours à la justice

115. L'article 10 du code civil dispose que « Chacun est tenu d'apporter son concours à la justice en vue de la manifestation de la vérité. Celui qui, sans motif légitime, se soustrait à cette obligation lorsqu'il en a été légalement requis, peut être contraint d'y satisfaire, au besoin à peine d'astreinte ou d'amende civile, sans préjudice de dommages et intérêts ».

Ce fondement a déjà été utilisé en justice, pour obliger les prestataires techniques à fournir les traces de connexion d'internautes à l'autorité judiciaire[57].

En outre, l'article 145 du nouveau code de procédure civile dispose que « *s'il existe un motif légitime de conserver ou d'établir avant tout procès la preuve de faits dont pourrait dépendre la solution d'un litige, les mesures d'instruction légalement admissibles peuvent être ordonnées à la demande de tout intéressé, sur requête ou en référé* ». Sur ce texte, le juge pourrait donc exiger d'un fournisseur d'accès à Internet ou d'un fournisseur d'hébergement de lui communiquer l'identité d'un utilisateur à partir des données de connexion le concernant. Seulement il doit exister un motif légitime de conservation : nous pourrons considérer qu'un motif légitime consistera en un acte manifestement illicite de la part d'un internaute.

Cette obligation d'apporter son concours à la justice a été appréhendée d'une manière plus précise et explicite en ce qui concerne les prestataires techniques.

[57] Voir l'ordonnance de référé du tribunal de commerce de Paris en date du 29 juin 2000

§2. Une obligation encadrée par des textes spécifiques

116. La loi n° 86-1067 du 30 septembre 1986, modifiée notamment par la loi du 1er août 2000, pose ce principe de divulgation des données de connexion aux autorités judiciaires dans son article 43-9 qui dispose que les prestataires sont tenus de fournir les données de nature à permettre l'identification de toute personne ayant contribué à la création d'un contenu de service (dont elles assurent la fourniture) aux autorités judiciaires qui en demandent la communication.

Cette obligation s'impose tant au fournisseur d'accès qu'au fournisseur d'hébergement : si un juge demande communication des données de connexion d'un internaute, les prestataires techniques doivent s'exécuter. La loi sur la confiance en l'économie numérique reprend cette disposition.

Il ne s'agit donc que d'une énonciation du principe déjà fort connu de l'article 10 du code civil.

CONCLUSION GENERALE

117. Les données de connexion des internautes sont aujourd'hui au cœur de l'actualité : contrefaçon en ligne, cyber-criminalité, presse et Internet… Les internautes, tous cyber-criminels[58] ?

Au-delà de ces interrogations, il faut toutefois se poser les questions fondamentales, de base : qu'est ce qu'une donnée de connexion ? Qui est l'internaute ? Quels sont les accès à ses données ? C'est à ces interrogations que nous nous sommes efforcés de répondre dans ce mémoire.

Ainsi à notre sens, les données de connexion sont les données qui permettent d'attester de la connexion d'un internaute sur Internet. Les données de connexion peuvent donc revêtir différents aspects : logs de connexion, cookies, variables de connexion, adresses IP… Toutes données attestant de la connexion donc, encore faut-il dire qui est l'internaute. L'internaute doit être considéré comme l'utilisateur du service et non pas comme l'abonné, bien que l'on présume ce dernier comme l'utilisateur.

Les données de connexion seront donc soumises à divers régimes juridiques - protection des données à caractère personnel, protection de la vie privée, protection de la correspondance privée… - et ces mécanismes permettront divers accès. Le cybernaute pourra actionner la protection des données à caractère personnel pour accéder aux données le concernant, et il pourra aussi accéder aux données de tiers lui portant atteinte.

Des tiers peuvent aussi accéder, collecter et traiter les données de connexion des internautes, que ce soit à des fins techniques, commerciales ou judiciaires… A ce propos, le débat actuel qui porte sur la musique en ligne est révélateur des antagonismes qu'il existe entre, d'une part, la protection qu'il faut accorder aux ayant droits et, d'autre part, la protection à conférer aux données de connexion des internautes.

Un équilibre, fragile mais nécessaire, doit être trouvé entre ces deux positions…

[58] Voir l'ouvrage de Olivier Iteanu, « Tous cybercriminels ? » aux Editions Jacques Marie Laffont

BIBLIOGRAPHIE

Ouvrages

Frayssinet, J. *Nouvelles technologies de l'information et de la communication et protection des libertés des consommateurs in les libertés individuelles à l'épreuve des NTIC*, PUL 2001

Fenoll-Trousseau, M.-P. et Haas, G. *Internet et protection des données personnelles*. Litec 2002

Lepage, A. *Libertés et droit fondamental à l'épreuve de l'Internet*, Litec, éditions du Juris-classeur 2002

Lucas, A., Devèze, J., et Frayssinet, J. *Droit de l'informatique et de l'Internet*, PUF

Vivant, M., Le Stanc, Ch. *Lamy Droit de l'informatique et des réseaux*, édition 2004

Articles

Aguado, A. *A propos de la directive 2002/58 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques*. Revue du droit de l'Union européenne, 2002, n°3, page 586, 1 page

Amouzou, P. *A propos du jugement du TGI de Paris du 15 janvier 2002, protection de la vie privée et des données personnelles : un spammeur enfin condamné...* Petites affiches du 1 août 2002, n°153, page 20, 1 page

Belloir, P. *L'application des règles de procédure pénale aux infractions commises sur le réseau Internet*. Expertises, 2002 ? n°262, page 293, 6

Bloch, F., Saulgrain, J., et Ruelle, J. *A propos du projet de loi relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la*

loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, aspects pratiques pour les entreprises « collectrices ». Legalis.net, 2001, n°3, page 79, 6 pages

Brabry E. *A propos du jugement du TGI de Paris, ordonnance de référé du 26 mai 2003, Informatique, Internet, Responsabilité de l'hébergeur*. Gazette du Palais du 24 septembre 2003, page 44, 2 pages

Barbry, E. et Lebon, H. *A propos de la directive n° 2002/58/CE du Parlement européen et du Conseil du 12 juillet concernant le traitement des données à caractère personne et la protection de la vie privée dans le secteur des communications électroniques, les cookies, les logiciels espions et la prospection commerciale par courriers électroniques prochainement réglementés*. Gazette du Palais du 20 avril 2003, page 14, 7 pages

Carpentier, Caroline. *Vie privée et communications électroniques, une union faite de compromis ?* www.droit-technologie.org. 2004

Dinant, Jean-Marc. *Les risques majeurs de l'IPv6 pour la protection des données à caractère personnel*. www.droit-technologie.org. 2001

Drouard, E. *Une culture « données personnelles », éclairage critique sur les communications électroniques*. Expertises, 2002, n°262, page 289, 4 pages

Drouard, E. *A propos de la directive européenne du 25 juin 2002, directive « communications électroniques » : la protection et la traçabilité en question*. Expertises, 2002, n°263, page 338, 3 pages

Dupuis, M. *La vie privée à l'épreuve de l'Internet : quelques aspects nouveaux*. Revue juridique personnes et famille, 2001, n°12, page 6, 4 pages

Ferchaud, B. *Les données personnelles, la loi et l'Internet*. Documentaliste sciences de l'information, 2002, volume 37, n°3-4, page 220, 3 pages

Frayssinet, J. *A propos de l'arrêt de la Cour d'appel de Paris du 30 janvier 2003, quand se mêlent le droit de la responsabilité civile et le droit de la protection des données personnelles*. Expertises, 2003, n°272, page 254, 4 pages

Frayssinet, J. *Le transfert et la protection des données personnelles en provenance de l'Union européenne vers les Etats-Unis : l'accord dit « sphère de sécurité » (ou safe harbour)*. Communication commerce électronique, 2001, n°3, chronique n°7, page 10, 5 pages

Frayssinet, J. *Le projet de loi relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel : constantes et nouveautés*. Communication commerce électronique, 2002, n°1, chronique n°1, page 11, 5 pages

Frayssinet, J. *Internet et l'obligation de sécurité des données personnelles*. Expertises, 2000, n°240, page 253, 4 pages

Gautier, P.-Y. *A propos de la directive CE du 12 juillet 2002, le droit au respect de la « vie privée » électronique est en marche*. Communication commerce électronique, 2002, n°10, Repères, page 2, 2 pages

Golvers, Luc. *L'informatique et la protection de la vie privée*. www.droit-technologie.org. 2001

Lalande, Sophie. *L'adresse IP de votre ordinateur : une donnée personnelle relevant du régime de protection communautaire ?* www.droit-ntic.com

Lemu, M. *Droit de copie, copie numérique, données publiques et données personnelles*. Documentaliste sciences de l'information, 2000, volume 37, n°2, page 121, 3 pages

Lepage, A. *Le secret de la vie privée sous influences*. Droit et patrimoine, 2002, n°102, page 61, 4 pages

Linglet, M. *Les technologies de l'information et la communication : boulimie de données personnelles*. Expertises, 1998, n°216, page 164, 1 page Maitrot de la Motte, Alexandre. *Le droit à la vie privée*. Groupe d'étude Société d'information et vie privée.

Lipovetsky, S et Yayon-Daudet, A. *Le devenir de la protection des données personnelles sur Internet*. Gazette du Palais du 12 septembre 2001, page 2, 9 pages

Meisse, E. *A propos de la directive du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques*. Europe, 2002, n°324, commentaire n°347, page 26, 1 page

Padova, Y. et Morel C. *Droit des fichiers, droit des personnes.* Gazette du Palais du 11 janvier 2004, page 2, 6 pages et Gazette du Palais du 9 avril 2004, page 2, 12 pages

Poidevin, B. *Le principe de l'effacement des données de connexion et ses exceptions*. Legalis.net, 2002, n°1, page 37, 4 pages

Rozenfeld, S. *L'Europe adopte l'opt-in mais n'interdit pas les cookies : le Parlement européen a enfin adopté une proposition de directive très attendue par le monde de l'Internet tant sur la question de la conservation des données de connexion que sur le « spam ».* Expertises, 2002, n°261, page 243, 1 page

Rozenfeld, S. *A propos du projet de loi sur l'économie numérique, un contenu dicté par les directives européennes.* Expertises, 2003, n°267, page 43, 1 page

Rozenfeld, S. *Le rapport Braibant sur la protection des données personnelles : moins de formalités et plus de pouvoirs pour la C.N.I.L*. Expertises, 1998, n°214, page 83, 1 page

Sitbon, C. *Données personnelles, quelle protection sur Internet ?* Legalis.net, 2001, n°2, page 64, 6 pages

Soulier J.-L., Slee, S. *La protection des données à caractère personnel et de la vie privée dans le secteur des communications électroniques : perspective française*. Revue internationale de droit comparé, 2002, n°2, page 665, 14 pages

Varet, V. *Les cadres juridiques du spam : Etats des lieux*. Communication commerce électronique, 2002, n°9, chronique n°21, page 14, 4 pages

Vivant, M., Mallet-Poujol, N., et Bruguière J.-M. *Informatique, droit de l'informatique, informatique et libertés*. JCP G, 2001, n°20-21, page 846, 2

Travaux universitaires

Egret, Benjamin. *Les problèmes juridiques des logiciels indiscrets*. Mémoire de DEA Informatique et Droit sous la direction du professeur Christian Le Stanc. 2001

Herbin, Cédric. *Les fournisseurs d'accès, les fournisseurs d'hébergement et les données personnelles*. Mémoire de DEA Informatique et Droit sous la direction du professeur Jean Frayssinet. 2003

Kassem, Hala. *L'internaute et son droit à être laissé tranquille*. Mémoire de DEA Informatique et Droit sous la direction du professeur Jean Frayssinet. 2003

Landrain, Pascal. *La lutte contre le spam*. Mémoire de DEA Informatique et Droit sous la direction du professeur Jean Frayssinet. 2003

Omarjee, Suliman. *Le data mining : aspects juridiques de l'intelligence artificielle au regard de la protection des données personnelles*. Mémoire de DEA Droit des créations immatérielles sous la direction du professeur Michel Bibent. 2002

Zeitoun, Stéphanie. *Le peer-to-peer*. Mémoire de DEA Informatique et Droit sous la direction du professeur Michel Vivant. 2003

Sites Internet

Association des fournisseurs d'accès : http://www.afa-org.fr

Clic Droit : http://www.clic-droit.com/

Droit NTIC : http://www.droit-ntic.com

Droit et nouvelles technologies : http://www.droit-technologie.org/

Juriscom : http://www.juriscom.net/

Jurisdata: http://www.juris-classeur.com/

Le forum des droits de l'Internet : http://www.forumInternet.org/

Legal Biznext : http://www.legalbiznext.com/

Legalis.net : http://www.legalis.net/

Les Petites Affiches : http://www.petites-affiches.com/

TABLE DES MATIERES