L'employeur : un fournisseur d'accès à l'internet comme les autres ?

Implications juridiques de la fourniture d'accès à l'internet par l'entreprise

Xavier LEMARTELEUR

DESS Expertise et Audit en Informatique et Techniques Numériques
UNIVERSITE PARIS II PANTHEON/ASSAS

Mémoire préparé sous la direction de M. Jean DONIO

Septembre 2003

Contact : xavier.lemarteleur@free.fr

Remerciements

Je tiens à remercier pour leurs enseignements, M. J. Donio ainsi que toute l'équipe professorale du DESS Expertise et Audit en Informatique et Technique Numériques.

Une attention particulière à ceux qui m'ont aidé dans la rédaction de ce mémoire :

M. F. Coupez, mon maître de stage durant cette année, pour ses conseils avisés, sa grande disponibilité et son soutien.

M. J. Zimmermann pour ses commentaires précieux sur le développement des points techniques.

Plan

Introduction

L'informatique est omniprésente dans notre vie quotidienne, le constat s'impose avec force : aucun domaine ne lui est plus étranger : les automobiles, les ascenseurs, les commutateurs téléphoniques, les systèmes de surveillance routiers mais aussi l'électroménager,… quasiment tous les secteurs de l'activité humaine sont envahis par les ordinateurs dans l'intimité du domicile comme dans la vie professionnelle.
Pourtant le temps qui nous sépare de la préhistoire informatique ne se compte pas en millions d'années mais en quelques décennies.

Les géants qui peuplaient l'univers informatique au début de son existence s'appelaient ENIAC[1] ou COLOSSUS[2] et à l'instar des dinosaures ils se caractérisaient par leur taille et leur poids considérable[3].

L'informaticien paléontologue n'a pas à rechercher les traces de ces géants disparus dans les strates profondément enfouies dans le sous-sol, en effet la préhistoire informatique ne remonte qu'a une cinquantaine d'années[4].
L'hégémonie de l'ordinateur s'est affirmée en un laps de temps extraordinairement court, jamais une (r)évolution technique n'aura connu un essor si rapide.

> De nos jours la puissance des ordinateurs est sans commune mesure avec celle des ancêtres qui les ont engendré, face aux quelques octets de mémoire dont disposaient les premiers calculateurs nos ordinateurs contemporains, même destinés au grand public, utilisent comme unité de décompte de la mémoire le giga octet; alors que la vitesse de fonctionnement de l'ENIAC était de 100 kilohertz, un processeur moderne dispose d'une fréquence de fonctionnement (fréquence d'horloge) de plusieurs gigahertz soit à peu près 20 000 fois plus rapide).[5]

Mais la nouvelle mutation majeure de l'informatique a fait de l'ordinateur une machine communicante ; en effet la possibilité de connecter des machines distantes a été une des dernières révolutions de l'ère numérique ; alors que déjà s'en annonce une nouvelle induite par la précédente : celle de la convergence des technologies[6].

---

[1] Pour Electronic Numerical Integrator And Calculator aussi dénommée machine Von Neumann conçu pour les calculs des tirs balistiques.

[2] Certains considèrent que Colossus Mark II, construit dès 1944 pour décrypter le Code généré par les célèbres machines Enigma, constituait le premier ordinateur avant l'ENIAC.

[3] L'ENIAC mesurait 30 mètres de long et 2.8 mètre de hauteur pour un poids de plus de 30 tonnes. Il utilise 18.000 tubes à vide, 70 000 résistances, 10 000 condensateurs et 6 000 commutateurs. L'aération nécessite des ventilateurs de 24 CV. La consommation électrique est de 150 kW (plusieurs rames de métro). Il occupe une surface de 1.000 mètres carrés. Multiplication en 3 millisecondes, fréquence d'horloge : 100kHz.

[4] L'ENIAC est né en 1946 à Philadelphie, université de Pennsylvanie.

[5] L'évolution de la puissance des ordinateurs est décrite par une loi énoncée en 1965 par G. Moore (dite loi de Moore) qui dit que *« le nombre de transistors d'un microprocesseur double tous les deux ans environs »*.

[6] *« La " grande convergence" qui rassemble l'informatique, les télécommunications, l'audiovisuel au sens large, est en cours. Cette convergence audiovisuel/Internet est largement entamée avec la numérisation de l'ensemble de la chaîne de valeur audiovisuelle, mais un pas supplémentaire sera franchi avec l'introduction future de la télévision numérique terrestre qui établira une équivalence réelle entre les anciens réseaux audiovisuels et ceux des télécommunications. »* C. Pierret, secrétaire d'Etat à l'industrie. Les 4èmes Entretiens de l'Autorité sous le haut patronage de Monsieur C. Poncelet, Président du Sénat. Internet et Télécommunications : les enjeux. 28 janvier 2000.

Cette révolution qui pratique l'unification des procédés techniques est permise notamment par les connexions à haut débit, tel est le cas de la télévision diffusée par des lignes de communication rapides comme les technologies de type xDSL[7].

Cependant cette avancée a été conditionnée par la naissance d'un réseau reliant les ordinateurs à l'échelle mondiale. Cette évolution est issue d'un projet expérimental du département de la défense américaine qui, en 1969, a conçu un système permettant la communication de données[8]. Il fut complété par le développement d'un protocole souple (TCP/IP) qui permit de créer un réseau fondé sur une architecture distribuée et non hiérarchique. A partir de cet « embryon » s'est développé un réseau mondial qui après de multiples mutations devint l'internet[9] tel que nous le connaissons de nos jours[10].
A l'origine l'internet regroupait principalement des chercheurs et universitaires (le réseau reliait les ordinateurs des différentes universités des Etats-Unis d'Amérique). Plus tard il s'ouvrit aux férus d'informatique, puis enfin au grand public qui voyait dans cet outil un moyen simple et efficace de communiquer ; finalement ce furent les entreprises qui prirent conscience de l'intérêt économique que pouvait avoir le réseau pour le développement de leurs activités.
Il représentait un moyen efficace d'assurer la communication au public comme vitrine publicitaire et outil de vente, plus encore il constituait un outil de travail performant permettant de communiquer quasiment instantanément par le biais des messageries électroniques (aussi dénommées e-mail)[11].

L'internet est vite devenu un enjeu stratégique pour les entreprises qui ont un important besoin de communiquer, comme le note le professeur Ph. le Tourneau : *« Le XXI^e siècle sera marqué, plus que tout autre dans l'histoire jusqu'à présent, par la communication, donc par la circulation des informations comme des connaissances. Et, dans une économie où les services ont pris le haut du pavé, les biens immatériels prédomineront. La source principale*

---

[7] Dont les plus connues sont l'ADSL acronyme de *asymetric digital suscriber line* et le SDSL *(symetric digital suscriber line)*.

[8] Le réseau ne s'appelait pas encore l'internet mais ARPANET.

[9] Le mot Internet vient de *Interconnected Network* qui peut être traduit par « interconnexion de réseaux » ; *« ... le mot 'internet' n'est pas une marque mais un nom générique qui, comme tel, doit recevoir un article (l'internet) et point de majuscules, exactement comme le téléphone, le minitel, la radio, le télex ou la télévision »*, Ph. le Tourneau, contrats informatiques et électroniques, éditions Dalloz, n° 4.
Mais aussi selon la recommandation de la commission des télécommunications (Commission générale de terminologie et de néologie) parue au J.O du 16/03/1999 (V. art. 11 du décret du 3 juillet 1996 relatif à l'enrichissement de la langue française), « internet », sans majuscule, est un nom masculin. Il convient donc de parler de « l'internet » comme l'on dit « le téléphone ». La définition donnée par la Liste est la suivante : *« Réseau mondial associant des ressources de télécommunication et des ordinateurs serveurs et clients, destiné à l'échange de messages électroniques, d'informations multimédia et de fichiers. Il fonctionne en utilisant un protocole commun qui permet l'acheminement de proche en proche de messages découpés en paquets indépendants. »*

[10] Pour plus de précisions : V. G. Cerf, *Technical writtings*. Disponible à l'adresse suivante : http://www.worldcom.com/resources/cerfs_up/technical_writtings.

[11] Selon la recommandation de la commission de l'informatique (Commission générale de terminologie et de néologie) parue au J.O du 20/06/2003, le message électronique (ou encore courrier électronique ou courriel) doit être défini comme *« un document informatisé qu'un utilisateur saisit, envoie ou consulte en différé par l'intermédiaire d'un réseau »*. Il est aussi précisé qu'*«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 ». »*

des richesses réside désormais dans les informations et les connaissances de tous ordres. Ce sont elles qui procurent aux entreprises des « avantages compétitifs ». [12]
On a donc vu, à une certaine époque, les sociétés consacrer une part importante de leurs ressources dans les systèmes d'information afin d'assurer leur présence sur l'internet.
Cette période se caractérisait par un engouement quasi frénétique pour tout ce qui était en relation avec l'internet et les nouvelles technologies, les investissements furent alors massifs dans ce secteur, on parlait de sociétés *« dot com*[13] *»*, de *« startup »* ou encore, en français, de « jeunes pousses » promises à un avenir radieux sur l'autel de la technologie. Les investisseurs, portés par cet engouement, firent littéralement exploser le cours de bourse des sociétés à peine créées, les valorisant à des montants astronomiques. Ce fut la désormais fameuse « bulle internet ».
Même si de nos jours la bulle a volé en éclats, en raison d'un marché économique finalement terriblement rationnel et pragmatique, les entreprises n'ont pas pour autant délaissé le réseau et continuent d'investir dans des architectures informatiques. L'internet continue donc de se développer sous l'initiative des sociétés mais aussi des particuliers et du monde associatif.

Mais si l'émergence de l'internet comme formidable vecteur de croissance économique, du moins pendant un temps, a permis d'étayer de nouveaux concepts économiques (comme le B to B, business to business, ou le C to B, consumer to business) décrivant les interactions possibles entre les acteurs du marché, le juriste, de son coté, y a vu un véritable défi en raison de la complexité juridique engendrée par cette immixtion des nouvelles technologies.

La naissance d'un réseau international, transfrontalier par nature, ne va pas sans quelques difficultés au plan juridique[14]. Le commerce se conciliant mal avec un univers chaotique et instable, en parallèle s'est développé un « droit du réseau » nécessaire pour appréhender ce nouveau monde encore inconnu. Il s'agissait d'abord pour les juristes d'adapter à l'internet le corpus de règles existant, ce ne fut que plus tard que le législateur intervint pour forger des normes propres au net[15].
La doctrine reste divisée, certains auteurs ont une approche « cessessioniste » considérant que le droit commun n'est pas applicable à l'internet et qu'il convient de créer des normes distinctes propres au réseau, d'autres estiment qu'il est plus opportun de ne pas favoriser l'inflation législative, et que les règles de droit commun sont applicables[16].
Dans ce chaos, on entend certains parler déjà d'une « *lex informatica* » qui serait une norme coutumière forgée par les acteurs de l'internet à l'instar de la « *lex mercatoria* »[17] que connaissent les marchands en droit international privé[18]. La régulation coutumière de

[12] Ph. le Tourneau, Folles idées sur les idées**,** Communication, Commerce électronique 2001/2, chron. 4.
[13] *« Dot com »* vient de l'extension du domaine internet « .com », le point se traduisant par *dot* en anglais.
[14] L'exemple caractéristique reste celui de l'affaire Yahoo/Licra relatif à la mise en vente d'objets nazis ayant donné lieu à deux décisions (ord. réf. Paris 22 mai 2000, Juriscom.net, http://www.juriscom.net/jpt/visu.php?ID=300, et TGI Paris 20 novembre 2000, Juriscom.net, http://www.juriscom.net/jpt/visu.php?ID=306). Ces décisions imposaient une obligation de filtrage à Yahoo ! inc. qui se heurta à une opposition des juridictions américaines.
[15] L'intervention du législateur se poursuit, on peut citer par exemple l'adoption en cours de la loi sur les communications électroniques et de la loi pour la confiance dans l'économie numérique.
[16] Sur ce point, P. Catala, actualité du droit de l'internet, Communication commerce électronique. Juin 2003.
[17] La validité de la *lex mercatoria* reste d'ailleurs très contestée en droit international privé.
[18] L'existence de règles coutumières est une réalité sur le réseau, ainsi le respect des principes de la « netiquette » est communément admis par l'ensemble des membres de la communauté des internautes. Cependant on peut s'interroger sur l'opportunité d'une telle régulation et sur sa portée. Pour consulter la

l'internet engendre un risque, celui de voir les acteurs puissants imposer leurs propres règles, il semble préférable que les normes applicables à l'internet soient édictées par un tiers extérieur (c'est-à-dire l'Etat bien qu'ici encore toute dérive ne soit pas exclue).

Le droit n'est pas encore fixé et continue d'évoluer pour s'ajuster à la nouvelle donne, alors que les évolutions techniques, rapides en informatique, contraignent le juriste à réagir parfois dans l'urgence.

Le droit appliqué aux technologies de l'information et de la communication (TIC) est donc un environnement mouvant, en perpétuelle évolution. Il en est ainsi du régime de responsabilité des acteurs de l'internet mais aussi des obligations pesant sur ceux-ci.
En effet l'architecture du réseau met en relation divers opérateurs : opérateurs de télécommunications, fournisseurs d'accès à l'internet (aussi dénommés sous l'acronyme FAI), d'hébergement, de contenus, … Chacun de ces intervenants remplit une fonction distincte et se voit appliquer des règles adaptées à son secteur d'activité.
Ces fonctions sont clairement énoncées dans l'avis du sénateur Türk sur le projet de loi relatif à la Confiance dans l'Economie Numérique :
« Plusieurs prestataires s'interposent, dans le cadre de la communication publique en ligne, entre l'auteur de l'information circulant sur Internet et son destinataire. Leur intervention, chacun à leur niveau, est indispensable pour que l'utilisateur d'Internet puisse accéder aux données présentes sur le réseau.
Le premier est l'opérateur. Il permet à l'utilisateur du service de communication publique en ligne de se connecter à une infrastructure (réseau téléphonique, réseau câblé) sur laquelle est diffusé l'Internet. Il a donc pour principale mission d'assurer la transmission de l'information.
Le fournisseur d'accès intervient, ensuite, pour mettre en relation ses abonnés avec les sites Internet ou les autres utilisateurs de l'Internet. A cette fin, il fournit, par le biais de contrats d'abonnement, des services de connexion à Internet ou des serveurs « proxy[19] ».
Le fournisseur d'hébergement a pour fonction de gérer techniquement les ressources connectées au réseau Internet et de mettre ces ressources à la disposition de ses abonnés. Il assure, en quelque sorte, une activité de loueur d'emplacement : techniquement, son rôle se résume à stocker sur son propre serveur l'ensemble des informations qu'il est conduit à recueillir et qui par la suite, seront consultées par les utilisateurs du service de communication publique en ligne.
L'éditeur (ou fournisseur) de contenus est un prestataire de services qui a pour fonction d'introduire de l'information sur un support logique ou physique, accessible par les utilisateurs de l'Internet.
Il convient néanmoins de souligner que, s'il est possible d'isoler juridiquement ces différents prestataires, en pratique, il peut y avoir confusion de plusieurs activités de prestations dans une même personne juridique. Ainsi, souvent, une même entité juridique exerce à la fois l'activité d'un fournisseur d'accès et d'un fournisseur d'hébergement. Parfois, elle est également, dans le même temps, fournisseur de contenus. De même, l'utilisateur de la communication publique en ligne (encore appelé, communément, l'internaute) n'est pas

---

netiquette : http://netiquette.afa-france.com/. L'AFA a également établi une liste d'exemples d'abus de service qui sont un autre élément de ce que pourrait être la *lex informatica* disponible à l'adresse : http://abuse.afa-france.com/.

[19] Voir glossaire des termes techniques en annexe.

toujours un simple consommateur de l'information diffusée en ligne ; il est aussi, dans certains cas, diffuseur d'informations sur Internet. »[20]

Une confusion des rôles est donc possible, il est ainsi fréquent que les fournisseurs d'accès soient aussi hébergeurs, mais il est aussi possible qu'un tiers devienne à ses dépens une acteur du réseau ; ainsi les grandes entreprises[21] disposant de milliers d'employés ont des besoins de connexion très importants et pourraient être amenées à se voir appliquer des mesures propres aux prestataires de l'internet. Ainsi s'il est facilement compréhensible que les entreprises disposant d'un site Web (une vitrine e-commerce par exemple) soient soumises aux obligations légales propres aux éditeurs (comme l'obligation de désigner le directeur de la publication) ou qu'une société étant son propre hébergeur se voit contrainte de conserver les données de connexion de la personne ayant mis en ligne un contenu[22], on imagine plus difficilement qu'elle soit soumise aux obligations généralement réservées aux fournisseurs d'accès internet.
Il en résulte une confusion des normes juridiques applicables aux acteurs, ce qui conduit à des situations contradictoires et parfois absconses.

Cela est encore accentué par le fait que le domaine reste fortement emprunt de considérations techniques, le juriste, non technicien, éprouvant parfois des difficultés à appréhender les enjeux techniques induits par l'évolution des technologies.

Afin de mieux cerner l'un de ces enjeux, il paraît donc nécessaire d'approfondir, en usant d'un vocabulaire plus technique[23] que nous efforcerons de rendre accessible au plus grand nombre, le fonctionnement pratique du réseau internet.

L'internet est un réseau fédérateur regroupant des réseaux hétérogènes. Cela implique que l'internet n'existe pas en tant que tel, il est en fait composé de multiples réseaux reliés entre eux par des lignes de communication rapides (on parle généralement de *« backbones*[24] *»*), que l'on pourrait les comparer à des autoroutes reliant de grandes villes.
Son fonctionnement est basé sur un protocole[25] (ensemble des règles nécessaires à la communication entre deux machines) baptisé TCP/IP[26] dont l'un des traits caractéristiques est son système d'adressage (IP pour *Internet protocol*).
Chaque machine présente sur le réseau dispose d'une adresse IP unique. Celle-ci prend la forme d'une série de 4 chiffres[27], par exemple : 125.21.36.2[28]. Cette adresse est un identifiant

---

[20] Sénat session ordinaire 2002-2003 Annexe au procès-verbal de la séance du 11 juin 2003, avis présenté au nom de la commission des Lois constitutionnelles, de législation, du suffrage universel, du Règlement et d'administration générale sur le projet de loi, adopté par l'Assemblée Nationale, pour la confiance dans l'économie numérique, par M. A. Türk, Sénateur.

[21] Notamment les entreprises du CAC 40 en raison de l'importance de leur parc informatique reliant en réseau des centaines voire des milliers d'ordinateurs.

[22] Disposition prévue par l'article 43-9 de la loi de 1986 sur la liberté de communication (mais dont l'application est sujette à controverse). Voir chapitre I B .p. 35.

[23] Il est parfois difficile pour le juriste d'appréhender sereinement un point technique, cependant même si il est « *souvent fâché dès le CE1 avec les sciences exactes, le juriste doit [donc] quitter sa crainte révérencielle à leur égard. »* J. E. Ray, de la sub/ordination à la sub/organisation, Droit Social, janvier 2002, n°1. p.9

[24] Voir glossaire des termes techniques en annexe.

[25] Voir glossaire des termes techniques en annexe.

[26] Il ne s'agit pas véritablement d'un seul protocole mais en réalité d'un ensemble de protocoles, ou parle ainsi de « pile TCP/IP ».

de la machine, à titre de comparaison on peut la rapprocher de l'adresse postale qui permet au facteur de distribuer son courrier, à une nuance près, en effet l'adresse IP peut être mouvante, il faudrait alors imaginer les vicissitudes du métier d'un postier dont le nom des rues ainsi que les numéros changeraient en permanence. Plus encore il en résulterait que personne ne pourrait comprendre l'adresse (savoir à qui elle correspond exactement), seul le bureau de poste local serait en mesure de déterminer à qui correspondait telle adresse à telle période donnée.

En effet l'adresse IP d'une machine peut être fixe (elle ne changera pas dans le temps) ou attribuée de manière dynamique (attribuée lors de chaque connexion). Ces adresses sont données par les fournisseurs d'accès qui les ont eux-mêmes obtenu de l'*Internet Assigned Numbers Authority* (IANA)[29].
Pour des raisons d'ordre pédagogique, en constatant que *« si les chiffres conviennent parfaitement aux ordinateurs, il n'en va pas de même pour les humains »*[30] a été mis en place un système permettant de faire correspondre l'adresse IP avec une adresse plus facilement mémorisable, ainsi l'adresse IP 125.21.36.2 s'écrira sous une forme plus aisément assimilable du type www.azerty.com.
C'est le *Domain name server* (DNS), un serveur qui garde en permanence la table des correspondances, qui se charge, de manière transparente pour l'utilisateur, d'assurer cette conversion. Ainsi lorsqu'il recevra une demande d'accès au site www.azerty.com il traduira la demande en un langage compréhensible pour la machine soit l'adresse IP (en l'espèce 125.21.36.2).

> Les données sur internet transitent sous forme de paquets (on parle de paquet IP). Le message à envoyer est dans un premier temps fractionné (c'est le rôle du protocole TCP). Chaque fragment du message sera ensuite encapsulé dans un paquet. Ces paquets comportent plusieurs informations comme l'adresse IP du destinataire, celle de l'expéditeur, des données de correction d'erreur. Selon les réseaux empruntés ces paquets pourront être à leur tour de nouveau encapsulés dans une trame. Enfin ces données vont circuler sur des lignes de télécommunications appartenant souvent à des opérateurs de télécommunications, bien que certains fournisseurs d'accès à l'internet aient développé leurs propres réseaux.

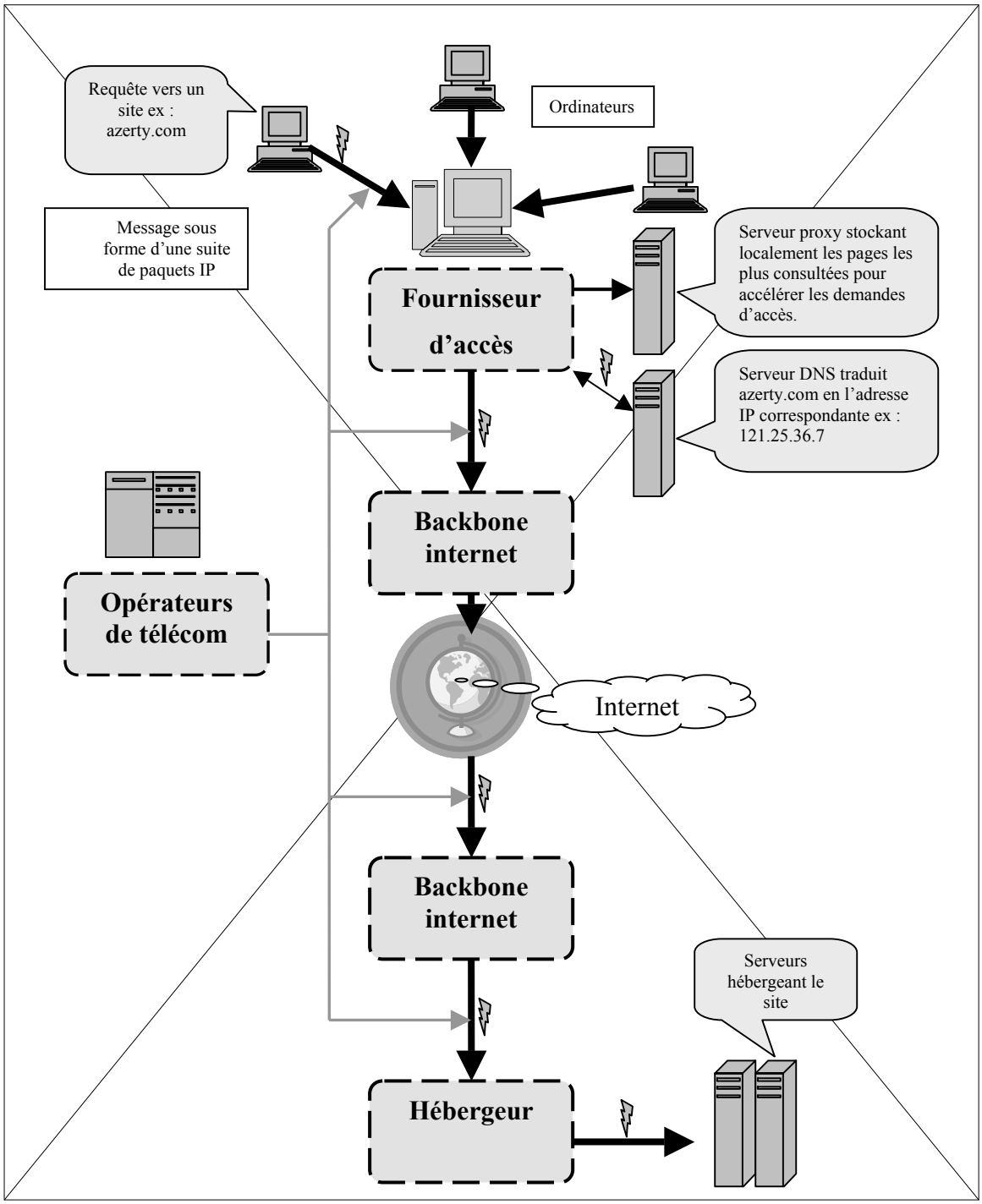
Le fonctionnement même du réseau induit la traçabilité de toute action faite sur le net (consultation d'un site, création de contenu,…) *« En effet, les protocoles de communication utilisés par Internet produisent des « traces » sur notre comportement ou nos habitudes qui sont détenues par des tiers, intermédiaires techniques, tels que les opérateurs de communication, les fournisseurs d'accès et les hébergeurs de sites. »*[31] Cette traçabilité a

---

[27] Cas des adresses IPv4 car l'adressage IPv6 qui commence à être implanté Code les adresses sur 128 bits.
[28] L'adresse est en fait codée sur 32 bits soit 4 fois un octet pour représenter des valeurs comprises entre 0 et 255.
[29] L'IANA délègue localement ses attributions. Ainsi ont été créés 4 *Regional Internet Registries* (RIR) : APNIC (région Asie/Pacifique), ARIN (Amérique du nord et Afrique sub-saharienne), LACNIC (Amérique latine et certaines îles des Caraïbes), et RIPE NCC (Europe, Moyen Orient, Asie centrale, Afrique au nord de l'équateur).
[30] V. Sédallian, Droit de l'internet. Éditions AUI, janvier 1997. p. 31. L'ouvrage est épuisé mais a été mis en ligne par l'auteur. Il est téléchargeable pour le consulter « à des fins non commerciales, notamment de recherche, d'éducation et d'enseignement » sur son site à l'adresse : http://www.internet-juridique/droitinternet.zip.
[31] CNIL, 21ème rapport d'activité 2000, éditions la Documentation Française. p. 22.

permis de justifier, en contrepartie, l'établissement d'un régime de responsabilité très atténué en faveur des acteurs du réseau.

On peut schématiser grossièrement une requête faite sur l'internet de la manière suivante :



La détermination de l'auteur d'un acte illicite sur le réseau implique donc que l'hébergeur du site conserve les adresses IP des machines ayant été à l'origine des demandes de connexions ; le lien entre l'adresse et une personne physique pourra être ensuite fait grâce aux données de connexion conservées par les fournisseurs d'accès. *« Ces données sont liées aux techniques utilisées sur internet pour établir la communication entre ordinateurs distants et à l'utilisation faite du réseau par l'individu ; elles concernent d'une part les adresses des machines du réseau, dites adresse IP, et en particulier celles de l'émetteur du message et de son destinataire, adresses auxquelles sont associées la date et l'heure de la connexion, des informations techniques caractérisant le type d'usage (accès au web, messagerie,..) d'autre part la requête (page du site que l'utilisateur veut visiter,…) ou le message proprement dit. Ces données sont collectées automatiquement par les fournisseurs d'accès et consignées dans un fichier dénommé « fichier log »*[32] .

Le terme de « données de connexions » recouvre en réalité tout un ensemble d'informations diverses. On peut les différentier selon trois catégories :

« 1. Les données de connexion simples. Elles sont générées chez le fournisseur d'accès à l'internet (FAI) : chaque fois qu'un abonné rentre sur le réseau, celui-ci doit donner le nom de compte et le mot de passe qui lui sont associés ; une fois que ces éléments ont été vérifiés, l'abonné se voit attribuer, pour la durée de la connexion, une adresse IP. Ces données rassemblent donc les éléments suivants : identité de l'abonné, heure de début de connexion, heure de fin de connexion, adresse IP qui a été attribuée à l'abonné durant cette connexion.
2. Les données de navigation, relatives aux sites internet visités ou aux services accédés par le titulaire d'une adresse IP connecté à un moment donné. Ces données sont générées par le fournisseur d'accès.
3. Les données de visite, générées sur les serveurs des sites internet visités, qui précisent les adresses IP des tiers qui ont visité ce site à un moment donné. »[33]

Cependant ce fragile équilibre peut être remis en cause en raison de l'évolution des technologies. On assiste en effet, suite au développement extraordinaire qu'a connu l'internet, à une pénurie des adresses IP[34], il a donc fallu trouver une parade pour faire face à cette situation.
La solution technique a consisté à faire correspondre plusieurs ordinateurs à une seule adresse IP. On parle ainsi de translation d'adresse connue sous l'acronyme NAT[35]. Il s'agit d'une fonctionnalité souvent incorporée dans les routeurs[36] (élément permettant l'acheminement des données sur un réseau) servant de passerelle[37] entre un réseau local

---

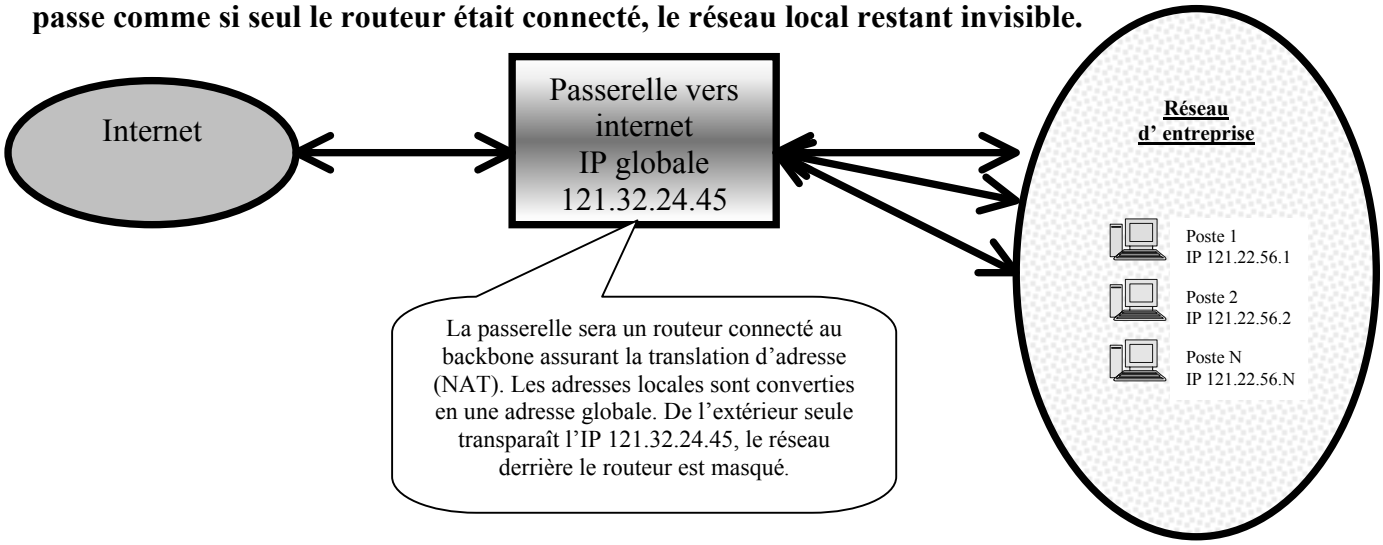
[32] Rapport du Conseil d'Etat, Internet et les réseaux numériques, adopté le 2 juillet 1998, éditions la Documentation Française.
[33] Définition issue de la consultation publique sur l'adaptation du cadre législatif de la société de l'information organisée par le ministère de l'économie et des finances (MINEFI).
[34] IPv4 autorise en théorie 4 milliards d'adresses possibles, mais en réalité certaines plages d'adressage sont réservées. Ce sont les adresses : 10.0.0.0 - 10.255.255.255 (10/8 prefix) ; 172.16.0.0 - 172.31.255.255 (172.16/12 prefix) ; 192.168.0.0 - 192.168.255.255 (192.168/16 prefix)
En conséquence, ces adresses ne sont pas routables (elles ne peuvent servir d'adresse valide sur le net) sur Internet et ne doivent pas être utilisées par des machines de ce réseau. Par contre, tous les réseaux privés peuvent utiliser ces adresses sans restrictions.
[35] *Network Address Translation.*
[36] Voir glossaire des termes techniques en annexe.
[37] Voir glossaire des termes techniques en annexe.

(comme un intranet[38] d'entreprise) et le réseau internet. Concrètement le principe revient à masquer les adresses IP des stations locales (les ordinateurs de l'entreprise par exemple) sous une adresse globale, le routeur NAT se chargeant de faire coïncider les deux. Les ordinateurs de l'entreprise n'auront que des adresses virtuelles, seule la passerelle disposera d'une adresse réelle.
La translation d'adresses comprend en fait plusieurs modalités[39] de fonctionnement, dont une en particulier mérite de retenir l'attention. Il s'agit du « NAPT MASQ » (*Network Address and Port Translation*). Il correspond au cas où plusieurs machines utilisent la même IP externe. Concrètement les ordinateurs qui se connecteront à l'internet auront la même adresse IP vu de l'extérieur, les machines ne sont pas visibles ou directement identifiables.

> La difficulté technique est de déterminer à quelle machine doivent être acheminés les paquets (puisqu'elles ont toute la même IP de destination à savoir celle de la passerelle).
> *Afin d'y parvenir le routeur va conserver tout un ensemble de données à savoir :*
> - ***l'adresse source*** *est le premier élément qui est regardé; chaque machine du réseau privé aura tendance dans la majorité des cas à communiquer avec une machine extérieure différente. Donc les paquets entrants seront porteurs de cette information et permettront au NAT d'identifier la machine à l'origine de chaque échange. Mais cela ne fonctionnera pas si les machines extérieures ne sont pas toutes différentes.*
> - ***le protocole supérieur*** *peut également être regardé par le NAT pour pouvoir identifier le contexte. Ce sera par exemple de l'UDP ou du TCP, et si une machine utilise le premier et une autre utilise TCP, alors le NAT saura retrouver la machine initiale de la connexion.*
> - ***le port*** *et d'autres informations liées aux protocoles supérieurs peuvent être utilisés pour identifier chaque contexte. Ainsi le NAT pourra faire la différence entre des paquets entrants qui présentent la même IP source, le même protocole de transport mais un port de destination différent*.[40]

[38] Voir glossaire des termes techniques en annexe.
[39] On peut aussi citer non exhaustivement :
Le NAT de base qui attribue statiquement une adresse IP à une autre il y a généralement dans ce cas autant d'IP privées qu'externes. La table de translation est alors fixe.
Le NAT dynamique qui attribue de manière dynamique (elle change dans le temps) une IP externe. Le routeur doit alors conserver la trace des changements effectués pour retrouver la station à l'origine de la requête, et pouvoir lui acheminer les informations demandées.
[40] Propos issus de sécuritéinfo.com. NAT.

Ainsi les stations locales, qui devraient normalement devoir disposer chacune d'une adresse unique sur internet, se verront attribuer une IP privée non routable (virtuelle), seul le routeur NAT disposera d'une IP routable (réelle) reconnue sur le réseau. Celui-ci masquera les IP privées pour les remplacer par la sienne. Vu de l'extérieur tout se passe comme si seul le routeur était connecté, le réseau local restant invisible.



L'utilisation de la fonctionnalité NAT a plusieurs conséquences au plan technique, elle permet ainsi de protéger un réseau contre des attaques venues de l'extérieur en le dissimulant de la vue des tiers ; par contre elle empêche l'établissement de certains type de connexions (certaines connexions sécurisées, trafic multicast,...) mais surtout elle *« casse le modèle IP de bout en bout : la perte de traçabilité de bout en bout rend la recherche impossible en cas de piratage provoqué par une machine interne. »*[41]
Cette dernière conséquence technique a un impact direct au niveau juridique car, comme on le verra, la responsabilité des acteurs de l'internet[42] repose principalement sur la possibilité de déterminer l'auteur du comportement illicite et donc sur les traces propres à toute connexion à l'internet. Or le NAT permet de masquer l'ensemble des ordinateurs situé à son amont. L'enjeu est de taille quand on sait que la technologie NAT est fréquemment utilisée pour relier les réseaux des grandes entreprises à l'internet et que ces infrastructures peuvent relier plusieurs centaines voire plusieurs milliers de machines[43].

> On peut arguer que le passage à Ipv6 sonnerait le glas du NAT en raison de la fin de la pénurie d'adresse, mais le NAT, qui se voulait une solution provisoire face à ce manque, a su prouver ses qualités, notamment en matière de sécurisation du réseau local (contre des attaques externes). Il y a donc peu de chance que cette technologie soit abandonnée dans un avenir proche.

[41] Cf la translation d'adresses : NAT ou IPmasquerade. Disponible à l'adresse suivante : http://secubook.tuxfamily.org.
[42] Voir infra développements relatifs à la responsabilité des acteurs de l'internet.
[43] Certaines sociétés ou groupes de sociétés disposent de plusieurs milliers d'ordinateurs en réseau et fournissent parfois l'accès à leurs sous-traitants. Pour cela ils disposent de un ou plusieurs points d'accès à très haut débit loués à des opérateurs. On peut penser principalement aux grands groupes du CAC 40.

Il conviendrait alors de conserver les fichiers logs[44] du routeur[45] NAT pour pouvoir rétablir la traçabilité de la même manière que les fournisseurs d'accès sont tenus de garder les données de connexion de leurs abonnés.

> Cette conservation des données de connexion est encore complexifiée sur le plan technique, par le fait que les routeurs ne disposent pas en général de mémoire de stockage de masse (disque dur). Il conviendrait alors d'utiliser un routeur logiciel installé sur un ordinateur disposant d'un espace disque conséquent ; et même ainsi il serait difficile de stocker ces données en raison du volume qu'elles peuvent représenter (sans doute plusieurs gigaoctets par jour dans le cas d'un réseau important).

Les législations applicables à l'internet tendant dans leur ensemble[46] à assurer la traçabilité des communications effectuées par les internautes, sont appelés à contribution les fournisseurs d'accès et les hébergeurs, en effet ceux-ci sont les seuls à pouvoir faire le lien entre une requête et un utilisateur. Il n'existe pas (ou du moins pas encore) de système centralisé permettant d'assurer cette traçabilité. Cependant le maintien de la possibilité de retracer les communications émises sur l'internet peut être remise en cause, notamment lorsqu'elles sont émises depuis un réseau d'entreprise utilisant un routeur NAT. Dans ce cas l'employeur doit-il être considéré comme un fournisseur d'accès et observer les dispositions légales afférentes ?

Il faudra, au vu des normes applicables à l'internet, déterminer les obligations reposant sur les acteurs du net en matière de conservation des données de connexion, pour les mettre en parallèle avec celles des entreprises (chapitre I).
Ensuite il s'agira de mettre en perspective ces obligations légales avec la législation régissant les rapports entre l'employeur et ses salariés (chapitre II).

[44] Voir glossaire des termes techniques en annexe.
[45] Voir glossaire des termes techniques en annexe.
[46] Il ne s'agit pas ici d'un apanage de la législation française mais d'une orientation ressentie au niveau mondial, cette impulsion a été grandement influencée par les attentats du 11 septembre. On peut citer à titre d'exemple le *« Patriot Act »* aux Etats-Unis ou en Grande Bretagne la loi *« Anti-terrorism, crime and security act »* ou encore au plan international « la convention sur la cybercriminalité ». Le ministre de l'intérieur britannique avait alors affirmé : *« les données concernant certaines personnes soumises à enquête ne seront disponibles que si les données concernant les communications de l'ensemble de la population sont conservées ».* Pour plus de détails, voir E. Wéry, L'internet sera-t-il le bouc émissaire des attentats du 11 septembre ? Les dangers au quotidien de la dérive sécuritaire, Expertises des systèmes d'information, n°257, mars 2002.

Chapitre I – L'internet à l'heure de la traçabilité : principe de conservation des données de connexion

La naissance d'un réseau informatique tel que l'internet offre des possibilités étendues en matière de contrôle de l'activité des citoyens. L'émergence d'un nouveau type de criminalité (dénommée cybercriminalité), facilitée par les moyens informatiques[47], a permis de justifier une surveillance sans commune mesure sur le net.

La lutte contre la cybercriminalité est devenue une préoccupation prépondérante des gouvernements des différents pays de la planète. Cette tendance s'est intensifiée après les attentats du 11 septembre aux Etats-Unis[48], la France n'étant pas une exception dans ce domaine.
Cette lutte passe par l'incrimination de divers comportements rendus possibles par l'interconnexion des systèmes d'information tels que : les intrusions, attaques de déni de service (denial of service ou DOS[49]), les infections par des virus[50] (et autres vers et troyens[51]) diffusion de contenus illicites (pornographie infantile, diffamations,…),... Le législateur avait vite pris conscience de l'enjeu que pouvait représenter les actes délictueux en matière informatique, ainsi la loi Godfrain du 5 janvier 1988[52] a inséré dans le Code pénal des mesures érigeant en infractions certains actes commis sur les systèmes d'information.
Mais en raison de l'émergence de l'internet, et de l'anonymat qu'il peut engendrer, il a fallu, afin de permettre la poursuite des auteurs de ces infractions, mettre en place des mécanismes pouvant assurer la traçabilité des connexions sur l'internet. Ces procédures reposent ainsi sur la coopération des intermédiaires du réseau. Pour la poursuite de cet objectif, il leur est imposé une obligation de conservation des données de connexion de leurs utilisateurs[53].

Ces dispositions sont inspirées par la crainte que nourrit dans l'inconscient collectif l'émergence d'un réseau international dans lequel ne régnerait que chaos et anarchie, fourmillant de mercenaires qui, à l'instar des pirates du temps jadis, seraient prêts à dévaliser le moindre innocent passant à leur portée.

Cependant ces mesures restent profondément liées au support numérique et aux possibilités de surveillance offertes par l'internet[54]. Dans notre civilisation moderne où la protection de la

---

[47] Et sans doute par l'apparent anonymat que procure l'internet.
[48] E. Wéry, L'internet sera-t-il le bouc émissaire des attentats du 11 septembre ? Les dangers au quotidien de la dérive sécuritaire, Expertises des systèmes d'information, n°257, mars 2002. précit.
[49] Voir glossaire des termes techniques en annexe.
[50] Voir glossaire des termes techniques en annexe.
[51] Voir glossaire des termes techniques en annexe.
[52] Loi relative aux atteintes aux systèmes de traitement automatisés de données n° 88-19 du 5 janvier 1988.
[53] Dès 1998 est apparue l'idée d'une nécessité de conserver les traces des connexions à l'internet au travers du rapport, précurseur en bien des points, du Conseil d'Etat. Il note ainsi : *« En outre, il importe de trouver un équilibre entre la préservation de l'anonymat des individus sur les réseaux et la nécessité de pouvoir retrouver leur identité lorsqu'ils commettent des infractions. Des obligations de conservation des données de connexion doivent dès lors être imposées aux intermédiaires techniques afin de faciliter les enquêtes judiciaires par une meilleure " traçabilité " des utilisateurs des réseaux ».* Internet et les réseaux numériques, Rapport du Conseil d'Etat adopté le 2 juillet 1998, éditions La Documentation française, p.16.
[54] Liées aux traces irrémédiablement laissées par toute connexion via le protocole TCP/IP utilisé sur l'internet.

vie privée et des libertés publiques est devenue un principe à valeur constitutionnelle[55], il serait impensable que la Poste se voit imposer une obligation de conservation des dates, heures, destinataires, expéditeurs et natures (carte postale, lettre manuscrite,…) des courriers émis, pourtant cette obligation existe en matière de communications électroniques par le biais de l'internet.

Ces diverses dispositions, en raison des limitations qu'elles peuvent apporter aux libertés, suscitent une certaine méfiance de la communauté des internautes[56] et une réaction notamment de la part des organismes en charge de la protection des données personnelles. Ainsi plus de cinquante autorités de protection des données et des commissaires à la protection de la vie privée ont remarqué, lors de la 24ème conférence internationale des commissaires à la protection des données qui s'est tenue à Cardiff du 9 au 11 septembre 2002, que : *« Alors qu'il est nécessaire de protéger la société des crimes tels que le terrorisme, la réaction de nombreux pays a été hors de proportion, et a eu de sérieuses implications sur la protection de la vie privée. Les commissaires estiment que la nécessité de protéger la vie privée à l'occasion de tels événements demeure une tâche essentielle pour la communauté internationale de protection des données. À moins que les gouvernements n'adoptent une approche qui prenne en compte les problèmes de protection des données personnelles à leur juste mesure, il est à craindre que ces gouvernements ne commencent à ébranler les plus fondamentales libertés, celles mêmes qu'ils cherchent à protéger »* [57].

Le citoyen internaute voit donc sa sphère de liberté se réduire en raison des tendances actuelles de nos législations : l'ordre et la sécurité publique tendent à prédominer sur les libertés individuelles[58].

On a donc vu se développer un ensemble de textes visant à assurer la traçabilité des connexions sur l'internet (A) ; cependant le cadre juridique ainsi créé demeure souvent imprécis quant au champ d'application et à la nature des obligations qu'il édicte. Ce flou législatif laisse la porte ouverte à nombre de suppositions, notamment quant à leur applicabilité aux réseaux d'entreprise (B).

---

[55] Et même réaffirmé au plan international, notamment par la Convention Européenne des Droits de l'Homme du 4 novembre 1950.

[56] Ainsi R. Stallman, fondateur de la Free Software Fondation, a pu déclarer : *« la vie privée est tout bonnement abolie lorsque les gouvernements surveillent ceux à qui vous parlez, où vous allez et ce que vous lisez »*.

[57] CNIL 23ème rapport d'activité 2002, éditions la Documentation Française. p. 38. Le rapport ajoute : *« les autorités de protection de l'Union européenne ont fait part, dans une déclaration rendue publique, de leur inquiétude concernant les propositions examinées au sein du Conseil de l'Union européenne qui auraient pour conséquence la conservation systématique et obligatoire des données de trafic relatives à l'usage de tout moyen de télécommunication (ex. : détails concernant la durée et le lieu des appels, les numéros utilisés pour téléphoner, envoyer un fax, un e-mail et les données relatives aux usages d'internet) pour une durée d'un an ou plus, afin d'en permettre l'accès aux autorités chargées de vérifier l'application effective de la loi. Elles ont également exprimé leurs doutes quant à la légitimité et la légalité de telles mesures tout en attirant l'attention sur leur coût excessif pour l'industrie des télécommunications et de l'internet,… »*

[58] C. Beccaria, qui a posé les bases de la réflexion pénale moderne, considérait que : *« les lois sont les conditions sous lesquelles des hommes indépendants et isolés se mirent en société. Fatigués de vivre dans un état de guerre continuel et dans une liberté rendue inutile par l'incertitude de la conserver, ils sacrifièrent une partie de cette liberté pour jouir du reste avec plus de sûreté et de sécurité ».* Cependant dans ce cas particulier on peut se demander si l'atteinte aux libertés n'est pas disproportionnée.

A. Un principe général : la conservation et l'accès aux données de connexion

L'année 2000 a été marquée par la mise en pratique du principe de conservation des traces de connexion. Les opérateurs de l'internet ont été amenés progressivement à conserver les données des personnes à qui ils fournissent l'accès à l'internet ou qui consultent les pages qu'ils hébergent. Ces dispositions sont complétées par diverses mesures permettant aux autorités judiciaires de prendre connaissance de ces données (2). Cette émergence d'une obligation de conservation des logs trouve son origine dans le régime de responsabilité des prestataires (1).

1. Origines de l'obligation de conservation

L'évolution du régime de responsabilité des prestataires de l'internet est étroitement liée à celle de leur devoir de collecte des traces de leurs usagers.
Alors qu'originellement elle semblait pouvoir être mise en cause aisément, les évolutions ultérieures ont montré que les opérateurs n'entendaient guère assumer la charge de la responsabilité liée aux actes de leurs utilisateurs[59].

Les premières décisions de justice mettant en cause la responsabilité des prestataires internet (sur le fondement de la responsabilité délictuelle issue des articles 1382 et 1383 du Code civil) furent marquées par une acceptation de leur rôle de la part de ces derniers. Du moins c'est ce qu'il ressort de la jurisprudence Calvacom[60] en date du 12 juin 1996. En l'espèce des prestataires (hébergeurs) avaient été mis en cause par l'UEJF au motif que certains des sites qu'ils hébergeaient comportaient des informations et des messages à caractère négationniste. Devant la complexité des débats le président du TGI demanda une médiation. Suite à cette médiation l'UEJF devait s'estimer *« en l'état et jusqu'à plus ample informée, remplie de ses droits à l'égard de toutes les défenderesses. »*

Dans leurs déclarations les hébergeurs, tout en essayant d'écarter leur responsabilité, considéraient que : *« la seule éventuelle responsabilité qui serait susceptible d'être recherchée à leur encontre devait être limitée aux seules pages web et forum de discussion dont elles sont les concepteurs, les animateurs et/ou qu'elles hébergent volontairement pour les diffuser soit pour leur propre compte, soit pour le compte d'un tiers, abonné ou annonceur, auxquelles elles sont contractuellement liées. »*
Les intermédiaires admettaient qu'il leur appartenait de fournir *« leurs meilleurs efforts »* pour limiter l'accès aux contenus illicites et qu'à défaut leur responsabilité pouvait être retenue.

---

[59] Sur la responsabilité des professionnels de l'internet, voir : H. Bitan, acteurs et responsabilité sur l'internet. Gazette du Palais, 1998.p.501 ; M. Vivant, la responsabilité des intermédiaires de l'internet, JCP, 1999, I. mais aussi, E. Barbry et F. Olivier, la responsabilité des professionnels de l'internet…une histoire sans fin …, Légicom n°21/22, 2000/1 P 79.

[60] Ord. Réf., Tribunal de Grande Instance de Paris, 12 juin 1996. UEJF contre CALVACOM et autres, Juriscom.net, http://www.juriscom.net/jpc/visu.php?ID=333.

Cependant deux mises en examen, mettant cette fois en cause des fournisseurs d'accès[61] pour diffusion d'images à caractère pédophile (sur le fondement de l'article 227-23 du Code pénal), la même année devaient attirer les critiques sur le régime de la responsabilité des acteurs de l'internet.
En réaction, la première tentative de régulation législative de la responsabilité des prestataires fut opérée par l'amendement Fillon (18 juin 96). Il proposait d'insérer dans la loi de 1986 sur la liberté de communication trois articles, parmi lesquels un était relatif à la responsabilité des fournisseurs d'accès, dont le contenu était le suivant :

> *« article 43-3 les personnes dont l'activité est d'offrir un service de connexion, ne sont pas pénalement responsables des infractions résultant du contenu des messages diffusés par un service de communication audiovisuelle auquel elles donnent accès si elles ont respecté les dispositions de l'article 43-1 et si ce service n'a pas fait l'objet d'un avis défavorable publié au Journal officiel en application de l'article 43-2, sauf s'il est établi que ces personnes ont, en connaissance de cause, personnellement commis l'infraction ou participé à sa commission ; »*

La première tentative de régulation, au travers de l'amendement Fillon, ne put aboutir en raison de la censure prononcée par le Conseil Constitutionnel[62]. En effet le texte prévoyait, au-delà du régime de responsabilité des fournisseurs d'accès, une obligation de filtrage des contenus (article 43-1) mais sans organiser de sanctions. L'article 43-2 instituait un organe d'autorégulation[63] : le Conseil Supérieur de la Télématique. Les articles 43-2 et 43-3 furent déclarés inconstitutionnels, en raison de la délimitation insuffisante des pouvoirs attribués au Conseil. L'inconstitutionnalité frappant l'article 43-2 fut étendue à l'article 43-3 déclaré inséparable. Seule subsistait la disposition concernant le filtrage des contenus par les fournisseurs d'accès.

Dans une seconde affaire impliquant un mannequin célèbre (Estelle H.[64]), le TGI, puis la Cour d'Appel de Paris reconnaissaient l'existence d'une responsabilité de l'hébergeur du fait des contenus qu'il héberge. En l'espèce, l'hébergeur Altern.org, représenté en la personne de V. Lacambre, abritait un site diffusant des photos intimes de Mme Estelle H. Faute de pouvoir déterminer l'auteur du site litigieux, la responsabilité de l'hébergeur fut engagée. Le juge retint que *« le fournisseur d'hébergement a l'obligation de veiller à la bonne moralité*

---

[61] Affaires *World net/ France net*, 7 mai 1996.
[62] Décision du 23 juillet 1996, Foruminternet.org, http://www.foruminternet.org/documents/jurisprudence/lire.phtml?id=233.
[63] Cette première démarche vers l'autorégulation marqua le commencement d'une réflexion qui fut poursuivie par un texte définissant ses principes fondateurs (« le Manifeste ») puis un ensemble de rapports : le rapport Beaussant de mars 1997, le rapport de Conseil d'Etat de 1998, le rapport de Paul de juillet 2000 (Du droit et des libertés sur Internet) pour aboutir en mai 2001 à la création du Forum des droits sur l'internet.
[64] Ord. Réf. TGI Paris 9 juin 1998 et Cour d'Appel Paris 10 février 1999, Estelle H. contre Altern.org. On peut aussi citer une affaire similaire : Lynda L., TGI Nanterre, 8 décembre 1999, Gaz. Pal., 11-12 février 2000, note H. Bitan, et ses développements : Cour d'Appel de Versailles 8 juin 2000, avec un infléchissement, le jugement de première instance est infirmé et la responsabilité de l'hébergeur écartée. Il convient de noter que cet arrêt intervint alors que les débats sur la loi 2000-719 étaient en cours et que la directive commerce électronique venait d'être adoptée. Voir L. Thoumyre, Responsabilité des hébergeurs : détours et contours de l'obligation de vigilance, Cahiers Lamy droit de l'informatique et des réseaux, nº127, juillet 2000, p. 5-9 ; également disponible sur Juriscom.net : http://www.juriscom.net/pro/2/resp20000805.htm.

de ceux qu'il héberge, au respect par ceux-ci des règles déontologiques régissant le Web et au respect par eux des lois et des règlements et des droits des tiers. »

Cette nouvelle condamnation devait entraîner une seconde réaction dans le monde politique, et donc une nouvelle tentative de régulation de la responsabilité des acteurs de l'internet. Après une première approche infructueuse faite par A. Madelin[65], ce fut l'amendement « Bloche »[66] qui fixa finalement les bases du régime actuel de la responsabilité sur l'internet.

> *« Art.43-8. - Les personnes physiques ou morales qui assurent, à titre gratuit ou onéreux, le stockage direct et permanent pour mise à disposition du public de signaux, d'écrits, d'images, de sons ou de messages de toute nature accessibles par ces services ne sont pénalement ou civilement responsables du fait du contenu de ces services que :*
> *- si, ayant été saisies par une autorité judiciaire, elles n'ont pas agi promptement pour empêcher l'accès à ce contenu ;*
> *- ou si, ayant été saisies par un tiers estimant que le contenu qu'elles hébergent est illicite ou lui cause un préjudice, elles n'ont pas procédé aux diligences appropriées. »*

Le troisième alinéa fut censuré par le Conseil Constitutionnel dans sa décision 2000-433 du 27 juillet 2000.

On assistait alors aux prémisses du principe de l'irresponsabilité des prestataires techniques, alors que la loi même commençait à établir un autre grand principe : celui de la conservation des logs.
Un régime de responsabilité limitée des acteurs techniques fut aussi instauré au niveau européen par la directive commerce électronique[67]. En effet celle-ci dispose que :

> ***Article 12 : Simple transport ("Mere conduct")***
> *1. Les États membres veillent à ce qu'en cas de fourniture d'un service de la société de l'information consistant à transmettre, sur un réseau de communication, des informations fournies par le destinataire du service ou à fournir un accès au réseau de communication, le prestataire de services ne soit pas responsable des informations transmises, à condition que le prestataire :*

---

[65] Son amendement, qui ne fut jamais déposé prévoyait : *« Art 43-2- Les personnes intermédiaires techniques, concourant à la mise en ligne sur les réseaux de télécommunications de services d'information, qu'ils soient transporteurs, fournisseurs d'accès ou fournisseurs d'hébergement, ne sont pas pénalement responsables des infractions résultant du contenu des messages diffusés par ce service de communication, sauf s'il est établi que ces personnes ont, en connaissance de cause, personnellement commis l'infraction, participé à sa commission, ou qu'ils n'ont pas accompli les diligences nécessaires à la faire cesser. »*

[66] Amendement déposé lors des débats sur la loi 2000-719 modifiant la loi de 1986 sur la liberté de communication.

[67] Directive 2000/31/CE du Parlement Européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur (« Directive sur le commerce électronique »). J.O.C.E., L 178/1 à 16 du 17 juillet 2000. La directive a d'ailleurs pu inspirer les divers amendements déposés en France en vue de réguler la responsabilité des prestataires de l'internet.

a) ne soit pas à l'origine de la transmission ;
b) ne sélectionne pas le destinataire de la transmission ; et
c) ne sélectionne et ne modifie pas les informations faisant l'objet de la transmission.
2. Les activités de transmission et de fourniture d'accès visées au paragraphe 1 englobent
le stockage automatique, intermédiaire et transitoire des informations transmises, pour autant que ce stockage serve exclusivement à l'exécution de la transmission sur le réseau de communication et que sa durée n'excède pas le temps raisonnablement nécessaire à la transmission.
3. Le présent article n'affecte pas la possibilité, pour une juridiction ou une autorité administrative, conformément aux systèmes juridiques des États membres, d'exiger du prestataire qu'il mette un terme à une violation ou qu'il prévienne une violation.

Article 13 : Forme de stockage dite "caching"
1. Les États membres veillent à ce qu'en cas de fourniture d'un service de la société de l'information consistant à transmettre, sur un réseau de communication, des informations fournies par un destinataire du service, le prestataire ne soit pas responsable au titre du stockage automatique, intermédiaire et temporaire de cette information fait dans le seul but de rendre plus efficace la transmission ultérieure de l'information à la demande d'autres destinataires du service, à condition que :
a) le prestataire ne modifie pas l'information ;
b) le prestataire se conforme aux conditions d'accès à l'information ;
c) le prestataire se conforme aux règles concernant la mise à jour de l'information, indiquées d'une manière largement reconnue et utilisées par les entreprises ;
d) le prestataire n'entrave pas l'utilisation licite de la technologie, largement reconnue et utilisée par l'industrie, dans le but d'obtenir des données sur l'utilisation de l'information ; et
e) le prestataire agisse promptement pour retirer l'information qu'il a stockée ou pour en rendre l'accès impossible dès qu'il a effectivement connaissance du fait que l'information à l'origine de la transmission a été retirée du réseau ou du fait que l'accès à l'information a été rendu impossible, ou du fait qu'un tribunal ou une autorité administrative a ordonné de retirer l'information ou d'en rendre l'accès impossible.
(...)

Article 14 : Hébergement
1. Les États membres veillent à ce que, en cas de fourniture d'un service de la société de l'information consistant à stocker des informations fournies par un destinataire du service, le prestataire ne soit pas responsable des informations stockées à la demande d'un destinataire du service à condition que :

a) le prestataire n'ait pas effectivement connaissance de l'activité ou de l'information illicites et, en ce qui concerne une demande en dommages intérêts, n'ait pas connaissance de faits ou de circonstances selon lesquels l'activité ou l'information illicite est apparente ; ou

b) le prestataire, dès le moment où il a de telles connaissances, agisse promptement pour retirer les informations ou rendre l'accès à celles-ci impossible.

2. Le paragraphe 1 ne s'applique pas lorsque le destinataire du service agit sous l'autorité ou le contrôle du prestataire.

3. Le présent article n'affecte pas la possibilité, pour une juridiction ou une autorité administrative, conformément aux systèmes juridiques des États membres, d'exiger du prestataire qu'il mette un terme à une violation ou qu'il prévienne une violation et n'affecte pas non plus la possibilité, pour les États membres, d'instaurer des procédures régissant le retrait de ces informations ou les actions pour en rendre l'accès impossible.

Le projet de loi pour la confiance dans l'économie numérique[68] reprend les dispositions issues de la directive[69] pour les transposer dans notre ordre juridique interne.

La limitation de la responsabilité des prestataires s'est développée de concert avec l'accroissement de leurs obligations de conserver les données de connexion de leurs utilisateurs.

L'intention sous-jacente de ces évolutions était de faire peser la charge de la responsabilité sur l'auteur réel du comportement illicite. Dans ce but il appartenait aux professionnels de l'internet d'apporter leur contribution en permettant l'identification des personnes ayant causé un trouble. Ce principe est affirmé par l'avis du sénateur Türk qui énonce qu' *« en limitant la responsabilité des intermédiaires techniques de la communication publique en ligne, le présent projet de loi fait porter l'essentiel de la responsabilité liée aux contenus illicites accessibles aux internautes sur les auteurs et éditeurs de contenus. Dans un tel contexte, il est donc essentiel que les auteurs puissent être identifiés, dans un souci de transparence de la communication publique en ligne. »*[70]

Les prestataires peuvent donc bénéficier d'une limitation de responsabilité dans la mesure où ils ont conservé les logs établissant une traçabilité des communications émises et reçues sur le net[71].

---

[68] Actuellement devant l'Assemblée Nationale en seconde lecture, projet n°991 : http://www.assemblee-nationale.fr/12/projets/pl0991.asp.

[69] Le projet de loi reprend les dispositions de l'article 14 de la directive dans le nouvel article 43-8 de la loi de 1986 et celle de l'article 12 et 13 de la directive dans les articles 32-3-3 et 4 nouveaux du Code des postes et télécommunications.

[70] Sénat session ordinaire 2002-2003, annexe au procès-verbal de la séance du 11 juin 2003, avis présenté au nom de la commission des lois constitutionnelles, de législation, du suffrage universel, du règlement et d'administration générale sur le projet de loi, adopté par l'Assemblée Nationale, pour la confiance dans l'économie numérique, par M. A. Türk, Sénateur. Précit.

[71] On peut d'ailleurs se demander si la traçabilité des internautes, pareillement à la viande bovine, n'est pas devenue une garantie de sécurité publique. Elle n'est pas le fait unique des gouvernements mais aussi, et cela est plus inquiétant, des groupes privés comme le note le sénateur Trégouët : « *Intel développe le projet T.C.P.A., Trusted computing platform alliance, soit « Alliance par une informatique de confiance ». Comment ne pas évoquer ici « le tiers de confiance » auquel nous aurions confié des clefs de déchiffrement dont la*

Les professionnels de l'internet ont donc voulu se dégager d'une responsabilité pesante pour être considérés comme de simples intermédiaires techniques. S'ils ont obtenu gain de cause c'est en contrepartie de la possibilité de déterminer l'auteur réel du comportement répréhensible au moyen de la conservation des logs.

C'est d'ailleurs se qui ressort du projet de loi pour la confiance dans l'économie numérique qui insère un article 79-7 dans la loi de 1986 sur la liberté de communication prévoyant qu' « *est puni d'un an d'emprisonnement et de 75.000 euros d'amende le fait, pour une personne physique ou le dirigeant de droit ou de fait d'une personne morale exerçant l'une des activités définies aux articles 43-7 et 43-8, de ne pas avoir conservé les éléments d'information visés à l'article 43-13 ou de ne pas déférer à la demande d'une autorité judiciaire d'obtenir communication desdits éléments.*
Les personnes morales peuvent être déclarées pénalement responsables de ces infractions dans les conditions prévues à l'article 121-2 du Code pénal. Elles encourent une peine d'amende, suivant les modalités prévues par l'article 131-38 du Code pénal, ainsi que les peines mentionnées aux 2° et 9° de l'article 131-39 du Code pénal. L'interdiction mentionnée au 2° de l'article 131-39 du Code pénal est prononcée pour une durée de cinq ans au plus et porte sur l'activité professionnelle dans l'exercice ou à l'occasion de laquelle l'infraction a été commise ».

Les mêmes peines sont prévues dans la loi sur la sécurité quotidienne (LSQ) concernant l'obligation de conservation qu'elle édicte (art. 39-3-1 du Code des postes et télécommunications).

A défaut de pouvoir déterminer l'auteur ayant mis en ligne des éléments litigieux le prestataire se voit infliger des sanctions importantes sous la forme d'une amende et de l'engagement de sa responsabilité pénale.
La fonction purement technique du professionnel de l'internet est reconnue, sa responsabilité ne pourra être engagée que s'il a commis une faute quasi intentionnelle en permettant l'accès à des contenus dont il avait connaissance du caractère illicite[72] ou qu'il a dépassé sa simple fonction technique[73]. Il est aussi responsable pénalement de la conservation des données de connexion de ses utilisateurs.

En conséquence on peut constater que le principe de non responsabilité des prestataires de l'internet reste conditionné par la détention des données de connexion des utilisateurs. En parallèle de l'affirmation de ce régime de responsabilité, favorable aux acteurs du net, les

---

sécurité eût été violée à la première réquisition. En effet, si ce projet est mené jusqu'à son terme, et il le sera inexorablement, tous nos ordinateurs seront dotés d'un des mouchards appelé – Fritz – en hommage au sénateur Fritz Holling qui se bat pour leurs généralisations ; votre ordinateur se bloquera si vous utilisez des logiciels qu'on vous aura prêtés ou si vos enfants ont chargé un film ou une musique sans avoir réglé les droits. L'ordinateur ne redémarrera qu'une fois votre situation régularisée. Les grands éditeurs de musique et de cinéma sont très favorables à un dispositif qui fera diminuer le piratage. Il suffit d'ajouter T.C.P.A. aux autres logiciels et systèmes d'exploitation développés par Microsoft comme Passport ou Palladium, pour mesurer les risques pour la liberté et la démocratie : de même que l'U.R.S.S. avait voulu répertorier toutes les machines à écrire et tous les fax, Microsoft tend à référencer tous les ordinateurs… ». Question du sénateur Trégouët lors des débats devant le Sénat du projet loi pour l'économie numérique.

[72] Dans le cas du fournisseur d'hébergement. Futur article 43-8 tel que prévu par le projet de loi pour la confiance dans l'économie numérique.

[73] Pour le FAI qui choisirait les destinataires ou serait à l'origine du message délictueux.

textes législatifs ont, en contrepartie et dans le même temps, instauré une obligation de conservation des données de connexion des utilisateurs.

2. Principes énoncés par la loi

La législation française, sous l'influence des directives communautaires et des conventions internationales, édicte une obligation imposant aux opérateurs de l'internet de conserver les données de connexion des personnes utilisant leurs services (a). Cette obligation est complétée par une possibilité de conservation des contenus visités au profit des autorités judiciaires (b).

a) La conservation des données de connexion

Il existe en France plusieurs textes législatifs imposant la conservation des logs. Historiquement, le premier fut la loi sur la communication audiovisuelle du 1er août 2000 modifiant la loi relative à la liberté de communication du 30 septembre 1986[74] qui comprend à son article 43-9[75] des dispositions imposant à certains prestataires de conserver les données pouvant permettre de retracer l'activité des internautes qui ont mis un contenu en ligne.
Cet article prévoit ainsi :

> « *Article 43-9* : *Les prestataires mentionnés aux articles 43-7* [personnes offrant l'accès] *et 43-8* [hébergeurs] *sont tenus de détenir et de conserver les données de nature à permettre l'identification de toute personne ayant contribué à la création d'un contenu des services dont elles sont prestataires.*
>
> *Ils sont également tenus de fournir aux personnes qui éditent un service de communication en ligne autre que de correspondance privée des moyens techniques permettant à celles-ci de satisfaire aux conditions d'identification prévues à l'article 43-10.*
>
> *Les autorités judiciaires peuvent requérir communication auprès des prestataires mentionnés aux articles 43-7 et 43-8 des données mentionnées au premier alinéa. Les dispositions des articles 226-17, 226-21 et 226-22 du Code pénal sont applicables au traitement de ces données.*
>
> *Un décret en Conseil d'Etat, pris après avis de la Commission nationale de l'informatique et des libertés, définit les données mentionnées au premier alinéa et détermine la durée et les modalités de leur conservation.* »

Il est ainsi créé une obligation de conservation des données de connexion. Concrètement, les opérateurs assurant l'accès et l'hébergement sur l'internet doivent détenir et conserver les

[74] Loi n° 86-1067
[75] Ce texte est sur le point d'être modifié par la loi pour la Confiance dans l'Economie Numérique actuellement en première lecture devant le Sénat.

traces permettant l'identification des personnes ayant participé à la création d'un contenu sur l'internet. Le texte renvoie à un décret[76] afin de déterminer les données devant être conservées, il semble que cela concerne, au minimum, l'adresse IP et les heures des connexions.

Prises en l'état, ces données ne constituent pas un moyen de retracer les actes d'un internaute sur le réseau. Mais mises en parallèle avec d'autres éléments dont les autorités judiciaires peuvent disposer, elles rendent désormais possible la relation entre une identité et un comportement constaté sur le net.

Le principe d'identification a, par la suite, été étendu par la Loi sur la Sécurité Quotidienne (LSQ), adoptée le 15 novembre 2001 dans un climat sécuritaire induit par les attentats survenus le 11 septembre.
Cette loi, instaurée à titre provisoire pour une durée de deux ans, vient d'être reconduite pour le même laps de temps. Ainsi « *originellement prévue jusqu'au 31 décembre 2003, l'application de ces mesures a été étendue, dans le cadre du projet de loi sur la sécurité intérieure, jusqu'au 31 décembre 2005* »[77]. Celle-ci contient certaines dispositions imposant la conservation des traces de connexion. La volonté du législateur était, comme nous avons pu le voir, de donner aux forces de sécurité les moyens indispensables à la lutte contre la cybercriminalité. Il convenait ainsi d'imposer une durée de conservation des données d'au moins un an et de disposer de logs suffisamment détaillés pour mener à bien les enquêtes[78].
Ainsi ont été insérées, à la fin du processus législatif[79], deux dispositions visant d'une part, à assurer l'anonymisation des données et, d'autre part, à organiser la conservation généralisée des traces de connexion. Ces dispositions sont contenues à l'article 29 de la LSQ[80].

Article 29 de la Loi sur la Sécurité Quotidienne :

> *« I. - Après l'article L. 32-3 du Code des postes et télécommunications, sont insérés deux articles ainsi rédigés:*
> *« Art. L. 32-3-1. - I. - Les opérateurs de télécommunications, et notamment ceux mentionnés à l'article 43-7 de la loi no 86-1067 du 30*

[76] Non encore paru à ce jour, ce qui ne va pas sans poser quelques difficultés d'application. Voir sur cette question dans ce même chapitre B) -2 p. 38.

[77] Forum des Droits sur l'Internet, rapport pour l'année 2002, la Documentation française, p.22. Il s'agit en fait de l'article 31 de la loi sur la sécurité intérieure qui dispose : *« L 'article 22 de la loi n° 2001-1062 du 15 novembre 2001 précitée est ainsi rédigé :*
Art. 22. - Les dispositions du présent chapitre répondent à la nécessité de disposer des moyens impérieusement nécessaires à la lutte contre le terrorisme alimenté notamment par le trafic de stupéfiants et les trafics d'armes et qui peut s'appuyer sur l'utilisation des nouvelles technologies de l'information et de la communication. Toutefois, les articles 24, 25 et 26 sont adoptés pour une durée allant jusqu'au 31 décembre 2005.
Le Parlement sera saisi par le Gouvernement, avant le 31 décembre 2003, d'un rapport d'évaluation sur l'application des dispositions du présent chapitre adoptées pour une durée allant jusqu'au 31 décembre 2005. Un second rapport lui sera remis avant le 31 décembre 2005 ».

[78] Sur ce point voir recommandation du Forum des Droits sur Internet du 18 décembre 2001, Conservation des données relatives à une communication électronique.

[79] En 2ème lecture devant le Sénat.

[80] Ces dispositions avaient initialement été incluses dans le projet de loi sur la société de l'information ou LSI (prédécesseur de la loi pour la confiance dans l'économie numérique) pour finalement être reprises dans la LSQ.

septembre 1986 précitée, sont tenus d'effacer ou de rendre anonyme toute donnée relative à une communication dès que celle-ci est achevée, sous réserve des dispositions des II, III et IV.
« II. - Pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales, et dans le seul but de permettre, en tant que de besoin, la mise à disposition de l'autorité judiciaire d'informations, il peut être différé pour une durée maximale d'un an aux opérations tendant à effacer ou à rendre anonymes certaines catégories de données techniques. Un décret en Conseil d'Etat, pris après avis de la Commission nationale de l'informatique et des libertés, détermine, dans les limites fixées par le IV, ces catégories de données et la durée de leur conservation, selon l'activité des opérateurs et la nature des communications ainsi que les modalités de compensation, le cas échéant, des surcoûts identifiables et spécifiques des prestations assurées à ce titre, à la demande de l'Etat, par les opérateurs. »
[...]

Ces nouvelles mesures marquent une généralisation de la conservation des logs, ne sont plus uniquement visées les personnes ayant créé un contenu, mais tout utilisateur indépendamment de son activité sur le net (simple consultation de sites, utilisation de la messagerie électronique,…). Cependant les données recueillies ne peuvent *« en aucun cas porter sur le contenu des correspondances échangées ou des informations consultées, sous quelque forme que ce soit »*[81]. Sont donc uniquement visées les données de connexion et non le contenu des pages visitées ou des messages échangés. Le principe de conservation, même s'il est accompagné d'une obligation d'anonymisation, est ici fortement étendu. Cette extension a d'ailleurs suscité quelques craintes de la part de la communauté des internautes et des organismes en charge de la protection de la vie privée[82].
En effet, pour la CNIL, *« la technologie d'Internet (c'est-à-dire le protocole de communication entre ordinateurs distants) permet déjà à certains robots de récupérer l'ensemble des adresses IP des ordinateurs connectés la conservation des données de connexion par les fournisseurs d'accès permettra d'identifier individuellement leurs utilisateurs ou tout au moins la personne physique titulaire de la ligne.*
De même, le rapprochement des données devant être conservées par les fournisseurs d'accès avec celles dont la loi du 1er août 2000 a prescrit la conservation aux hébergeurs de sites, permettrait d'identifier, non pas seulement les personnes ayant rendu un contenu accessible

[81] Article 32-3-1. IV, du Code des postes et télécommunications introduit par la LSQ.
[82] Comme par exemple la CNIL qui, dans son avis sur la loi sur la société de l'information, notait : *« Il convient d'emblée de relever qu'en faisant obligation aux opérateurs de télécommunications de conserver des données de connexion dépourvues d'utilité pour la facturation, le projet de loi ne poursuit pas un objectif d'ordre public qui serait justifié par la nécessité d'identifier les auteurs de contenus illégaux ou attentatoires aux droits des tiers (sites pédophiles, négationnistes, racistes, diffamatoires et autres). En effet, la loi du 1er août 2000 a déjà établi à la charge des hébergeurs de sites mais aussi des fournisseurs d'accès — visés ensemble par l'article 43-9 nouveau de la loi du 30 septembre 1986 — une obligation générale de « détenir et conserver les données de nature à permettre l'identification de toute personne ayant contribué à la création d'un contenu », dans des conditions et pour une durée qui doivent être précisées par un décret en Conseil d'Etat pris après avis de la CNIL, les données ainsi conservées pouvant être requises par l'autorité judiciaire. Le projet de loi sur la société de l'information est de portée beaucoup plus large puisqu'il concerne tous les internautes qui échangent des mails ou naviguent sur le Web, même s'ils ne créent aucun contenu accessible au public. »*

sur Internet, mais beaucoup plus généralement les internautes s'étant bornés à consulter tel ou tel site»[83].

L'extension du principe de conservation des données de connexion devait encore être affirmé une nouvelle fois au travers d'un « cavalier budgétaire[84] » inclus dans la loi de finances rectificatives pour l'année 2001[85] (dite LFR 2001).
Ainsi l'article 62 de la LFR 2001 permet également, aux agents des douanes et aux enquêteurs de la COB d'obtenir communication des données conservées par les entreprises visées par la LSQ (fournisseurs d'accès) mais elle introduit une confusion sur la nature des prestataires sur lesquels pèse l'obligation. En effet la loi vise ici *« les opérateurs de télécommunication et les prestataires mentionnés aux articles 43-7* [personnes offrant l'accès] *et 43-8* [hébergeurs] *de la loi no 86-1067 du 30 septembre 1986 relative à la liberté de communication ».* Alors que le texte de la LSQ ne visait que les personnes permettant l'accès à l'internet, le texte de la LFR semble étendre l'obligation aux hébergeurs (les entreprises qui exercent la fonction d'hébergeur seraient alors explicitement visées).

L'analyse des textes laisse apparaître une tendance conduisant à l'élargissement de l'obligation de conservation des « logs ». Successivement la loi relative à la communication audiovisuelle, la LSQ puis la LFR 2001 ont étendu les mesures visant à la conservation des données de connexion. Il est probable que cette tendance soit amenée à se poursuivre au fil de l'évolution législative.

Ce principe de conservation des traces demeure cependant sujet à certaines interrogations. En effet, les textes imposant la conservation des données de connexion, sous une apparente clarté, comportent des zones obscures qui ne permettent pas de déterminer avec précision le champ d'application effectif des mesures prescrites.

La loi de 2000 modifiant la loi sur la liberté de communication de 1986, de même que les dispositions de la LSQ prévoient le recours à un décret pris en Conseil d'Etat pour délimiter la durée, les modalités et la nature des données à conserver. Ainsi l'article 43-9 établissant une obligation de conservation des logs de toute personne ayant participé à la mise en ligne d'un contenu dispose dans son dernier alinéa qu' « *un décret en Conseil d'Etat, pris après avis de la Commission nationale de l'informatique et des libertés, définit les données mentionnées au premier alinéa et détermine la durée et les modalités de leur conservation. »*

Il appartient donc à l'autorité réglementaire de fixer le périmètre exact de la loi. Deux points cruciaux sont ici concernés, à savoir la nature des données devant être conservées et la durée de cette conservation. En l'absence de telles précisions le texte ne semble pouvoir être appliqué.
La jurisprudence a récemment du se prononcer sur l'application de l'article 43-9 en l'absence de décret de transposition.
Suite à la diffusion de textes à caractère xénophobe, deux organismes luttant contre le racisme avaient assigné une association (Edaama.org) qui fournissait un hébergement gratuit

[83] CNIL, 20ème rapport d'activité 2000, avis concernant le projet de loi sur la société de l'information.
[84] Un cavalier budgétaire est une disposition incluse dans une loi de finance alors même que cette disposition ne concerne pas directement les finances publiques.
[85] Loi de finances rectificative pour 2001 n° 2001-1276 du 28 décembre 2001.

et la société OVH à laquelle Edaama avait loué un espace de stockage disque. Les requérants demandaient notamment la transmission des journaux de connexion. Le Tribunal de Grande Instance de Paris, saisi par voie de référé, a donc été amené à déterminer si les dispositions de l'article 43-9 étaient applicables. L'ordonnance de référé[86] tranche la question de manière ambiguë ; elle estime d'abord qu'il existe une *« sérieuse contestation quant à la portée de l'obligation »* faite aux hébergeurs de détenir et de conserver les données de connexion. Le tribunal remarque en effet que *« la nature des données d'identification, comme les modalités de leur conservation, devrait, suivant les dispositions de l'article 43-9 de la loi du 1er août 2000, être précisée par un décret en Conseil d'Etat, non encore publié, après avis de la Commission Nationale de l'Informatique et des Libertés »* et qu'il ne peut y avoir d'obligation pour OVH de transmettre les données de connexion. Dans un second temps, elle estime qu'il appartient à Edaama (qu'elle refuse de qualifier d'hébergeur) de communiquer aux demanderesses les informations *« relatives aux circonstances, notamment de temps, de la mise en ligne des écrits constituant le trouble illicite, et permettant d'identifier toutes personnes ayant contribué à leur création y compris sous forme d'extraits des journaux de connexions qui y sont relatifs »* sous astreinte de 3000 euros par jour. Il semblerait donc que les dispositions de l'article 43-9 ne soient pas applicables en l'absence de promulgation du décret d'application.
Il est surprenant de constater que, plus de trois ans après son adoption, le pouvoir réglementaire n'a pas encore estimé bon de prendre les mesures qui relèvent de sa compétence pour que cette disposition soit enfin effective, alors que le projet de loi pour la confiance dans l'économie numérique est sur le point de réformer l'article 43-9.

Parallèlement, la loi sur la Sécurité Quotidienne, comme il a été vu précédemment, ordonne la conservation des logs relatifs à toute connexion faite sur l'internet. Là aussi le texte laisse au pouvoir réglementaire le soin de préciser les modalités régissant cette conservation. Il est prévu qu' *« un décret en Conseil d'Etat, pris après avis de la Commission nationale de l'informatique et des libertés, détermine, dans les limites fixées par le IV, ces catégories de données et la durée de leur conservation, selon l'activité des opérateurs et la nature des communications ainsi que les modalités de compensation, le cas échéant, des surcoûts identifiables et spécifiques des prestations assurées à ce titre, à la demande de l'Etat, par les opérateurs.*[87] *»*
Ici encore les autorités administratives n'ont pas pris le soin d'adopter les mesures nécessaires à l'application de ces dispositions.
On peut donc tout naturellement s'interroger sur les raisons justifiant cette absence d'action[88], alors que l'adoption de ces textes a été l'occasion de vives critiques de la part des groupes d'utilisateurs et de certaines autorités administratives, au premier rang desquelles figure la CNIL. Ce retard trouve peut-être une de ses explications dans les divergences qui opposent le gouvernement et la CNIL sur la durée de conservation des logs[89].

---

[86] Ord. réf. TGI Paris 26 mai 2003, Juriscom.net, http://www.juriscom.net/jpt/visu.php?ID=232 ; L. Thoumyre, Affaire OVH : "contestation sérieuse" sur l'obligation faite au hébergeurs de détenir les données de connexion, Juriscom.net, actualités, http://www.juriscom.net/actu/visu.php?ID=233.
[87] Article 32-3-1 du Code des postes et télécommunications *in fine*.
[88] Le cas français n'est pas isolé, parmi les autres états ayant adopté une législation similaire, nombres d'entre eux n'ont pas pris les mesures nécessaires en vue de leur applicabilité. Voir sur ce point, Forum des droits sur l'internet, Premier rapport d'activité, année 2002. p. 21.
[89] On peut aussi penser que le gouvernement a souhaité attendre l'entrée en vigueur de la convention cybercriminalité pour promulguer les décrets d'application.

Il serait donc bon que le périmètre des obligations soit enfin clairement défini. L'inaction du gouvernement n'est pas pour favoriser la sécurité juridique : en absence de dispositions légales valides, les prestataires ont dû unilatéralement mettre en place une politique de conservation des données de connexion[90]. Ainsi l'Association Française des Fournisseurs d'Accès et de services internet (AFA), regroupant une très grande part des FAI exerçant leurs activités en France, a adopté un texte intitulé « Pratiques et Usages des Membres de l'AFA ». Ce texte, qui n'a pas de valeur légale en tant que tel et ne constitue donc qu'un simple Code de bonne conduite, prévoit la conservation des données de connexion au point 2.5.

> ***2.5 Conservation des données de connexion de l'Utilisateur***
>
> *Les données suivantes sont conservées, sous réserve d'éventuels aléas techniques :*
> ***2.5.1 Par le fournisseur d'accès***
> *Les données de connexion à Internet comprennent les éléments suivants : login de l'Utilisateur, adresse IP qui lui est affectée, date et heure exactes de connexion, date et heure exactes de déconnexion.*
> *La durée de conservation la plus courante des fournisseurs d'accès membres de l'AFA est de trois mois.*
> ***2.5.2 Par l'opérateur de serveurs caches***
> *Certains fournisseurs d'accès opèrent des serveurs caches afin d'accélérer la consultation des données sur le réseau.*
> *Les données de connexion aux caches comprennent les éléments suivants : adresse IP de l'Internaute, identification du serveur requis par l'Utilisateur, document demandé, date et heure exacte.*
> *La durée de conservation la plus courante des membres de l'AFA opérant des serveurs caches est de trois à cinq jours.*
> ***2.5.3 Par l'hébergeur***
> *Les données de mise à jour du contenu hébergé comprennent les éléments suivants : login de l'Utilisateur, adresse IP qui lui est affectée par son fournisseur d'accès, date et heure exactes de connexion, date et heure exactes de déconnexion.*
> *La durée de conservation la plus courante des hébergeurs membres de l'AFA est de trois mois.*

Les prestataires ont donc préféré parer à l'incertitude juridique en adoptant une position prudente en matière de conservation des logs.

Au-delà du principe de détention de ces traces de connexion (qui ne concerne pas les contenus visités), la législation, afin de donner des moyens complémentaires aux autorités judiciaires dans leur lutte contre la criminalité informatique, a prévu la possibilité d'ordonner la conservation des contenus consultés.

[90] Les fournisseurs d'accès, au travers de l'AFA, ont même anticipé sur les obligations législatives, en

b) La conservation des contenus

Les autorités judiciaires se sont vues accorder la possibilité d'ordonner, à certains acteurs de l'internet, la rétention des contenus dans des cas particuliers.
Il en est ainsi du nouvel article 60-1 du Code de procédure pénale instauré par la loi sur la Sécurité Intérieure qui permet à l'autorité judiciaire d'ordonner, aux opérateurs de télécommunication notamment, de conserver les données concernant le contenu consulté par un utilisateur du net.
Le nouvel article 60-1 du Code de procédure pénale dispose donc que (extraits) :

> *«… L'officier de police judiciaire, intervenant sur réquisition du procureur de la République préalablement autorisé par ordonnance du juge des libertés et de la détention, peut requérir des opérateurs de télécommunications, et notamment de ceux mentionnés à l'article 43-7 de la loi n° 86-1067 du 30 septembre 1986 relative à la liberté de communication, de prendre, sans délai, toutes mesures propres à assurer la préservation, pour une durée ne pouvant excéder un an, du contenu des informations consultées par les personnes utilisatrices des services fournis par les opérateurs…. »*[91]

Dans le prolongement de ce texte un projet de loi, adopté en première lecture par l'Assemblée Nationale, vient encore renforcer le contrôle en permettant aux autorités judiciaires de prendre connaissance de correspondances adressées par le biais de réseaux de télécommunication (notamment l'internet). Il introduit ainsi dans le Code de procédure pénale un nouvel article :

> *« Art. 706-96. - Si les nécessités de l'enquête de flagrance ou de l'enquête préliminaire relative à l'une des infractions entrant dans le champ d'application de l'article 706-73 l'exigent, le juge des libertés et de la détention du tribunal de grande instance peut, à la requête du procureur de la République, autoriser l'interception, l'enregistrement et la transcription de correspondances émises par la voie des télécommunications selon les modalités prévues par les articles 100-1 et 100-3 à 100-7, pour une durée maximum de quinze jours, renouvelable une fois dans les mêmes conditions de forme et de durée. Ces opérations sont faites sous le contrôle du juge des libertés et de la détention.*
> *«Pour l'application des dispositions des articles 100-3 à 100-5, les attributions confiées au juge d'instruction ou à l'officier de police judiciaire commis par lui sont exercées par le procureur de la République ou l'officier de police judiciaire requis par ce magistrat.*

prévoyant la conservation des données de connexion depuis 1998 soit deux ans avant la loi 2000-719.

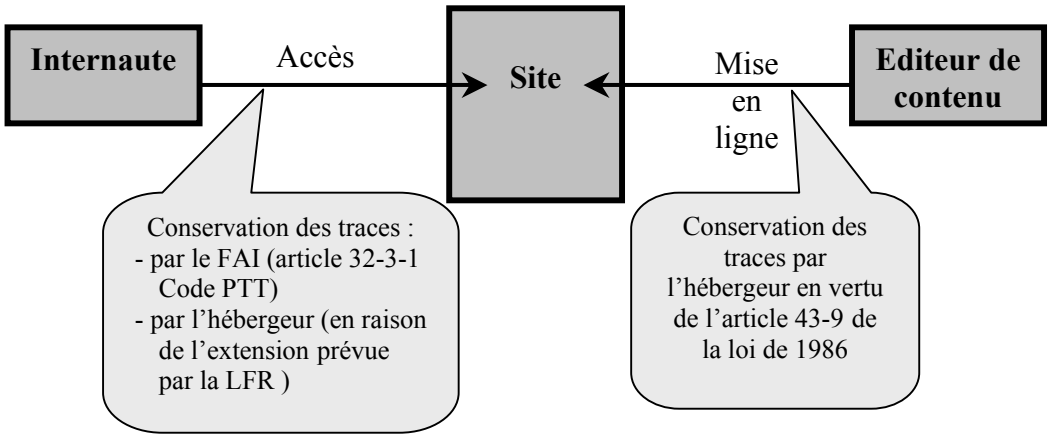
[91] Article 18 de la loi sur la Sécurité Intérieure

«Le juge des libertés et de la détention qui a autorisé l'interception est informé dans les meilleurs délais par le procureur de la République des actes accomplis en application de l'alinéa précédent »[92]

Ces mesures viennent compléter les dispositions relatives à la conservation des données de connexion en les étendant aux informations relatives aux contenus consultés et aux correspondances émises par le biais de l'internet. Les possibilités en matière de contrôle offertes aux autorités judiciaires se trouvent ainsi considérablement étendues.

On peut donc, pour résumer l'état de la législation française en matière de conservation des données de connexion, constater que :

- premièrement les données relatives à l'identification de toute personne ayant contribué à créer un contenu sur l'internet[93] mais aussi de celles ayant simplement utilisé le réseau[94] doivent être conservées[95].
- deuxièmement les informations relatives au contenu des sites visités[96], mais aussi celles concernant le contenu des correspondances échangées[97], peuvent, sur requête de l'autorité judiciaire, être conservées par les opérateurs du réseau.



[92] Projet loi Perben portant adaptation de la justice aux évolutions de la criminalité adoptée en première lecture par l'Assemblée Nationale.
[93] Article 43-9 de la loi de 1986 sur la liberté de communication.
[94] Article 32-3-1 du Code des postes et télécommunications inséré par la LSQ.
[95] Il existe deux obligations distinctes, la première est liée à la création d'un contenu sur l'internet, la seconde, autonome, concerne les données de connexion des internautes ayant simplement visité des sites. La seconde ne consiste pas uniquement en un élargissement de la première. Les données conservées ne seront pas forcément identiques dans les deux cas. *Contra,* Türk, avis sur le projet de loi pour la confiance dans l'économie numérique qui considère qu' «*en tout état de cause, l'obligation de conservation de données d'identification prévue à cet article reprend, en l'élargissant, le contenu d'une obligation déjà prévue, à l'égard des seuls fournisseurs d'accès, par l'article L. 32-3-1 du Code des postes et télécommunications.*
[96] Article 60-1 du Code de procédure pénale inséré par la loi sur la sécurité intérieure.
[97] Futur article 706-96 du Code de procédure pénale inséré par la loi portant adaptation de la justice aux évolutions de la criminalité.

Le panel de moyens à la disposition des autorités d'enquête est très large, il permet facilement de retracer tout agissement frauduleux commis par un utilisateur sur l'internet. On peut cependant montrer une certaine inquiétude face à la portée de ces mesures qui, associées, pourraient permettre une surveillance très précise des actions des internautes.

Notons toutefois que les décisions prises au niveau local par les différents états sont issues de dispositions supranationales. Ainsi la convention sur la cybercriminalité[98], adoptée au sein du Conseil de l'Europe[99] signée à Budapest le 23 novembre 2001[100] comporte des dispositions similaires en matière de conservation des données de connexion. Ce texte a grandement orienté les législations des états signataires[101]. Elle résulte d'une prise de conscience que la lutte contre la criminalité numérique, transfrontalière par nature, nécessite un travail coordonné et concerté entre les Etats[102] au-delà des efforts consentis localement par les différents pays.
La convention a donné les orientations que devaient suivre les états membres notamment relativement à la collecte des données informatiques. Selon les articles 16 et 20 :

[98] Cette convention n'est pas le seul élément marquant les préoccupations internationales en matière de lutte contre la criminalité numérique, des discussions ont été engagées et des groupes de travail ont aussi été constitués dans le cadre du G8 (organisation regroupant les pays les plus industrialisés de la planète). Lors de la réunion du G8 au Canada (Mont Tremblant) en 2002 les participants convenaient qu' *« afin de prévenir les activités criminelles et terroristes, d'intenter des poursuites et de faire enquête, le cas échéant, les forces de l'ordre doivent avoir un accès légal aux données d'achalandage et aux renseignements sur les abonnés dont disposent les fournisseurs de services de communications. Toutefois, les enquêtes sur les activités criminelles et terroristes sont de plus en plus entravées par l'absence de ces données et renseignements. »*

[99] Des états non membres ont été associés à cette convention : les Etats Unis, le Japon, l'Afrique du sud et le Canada.

[100] Il est intéressant de noter que la convention, dont le premières bases avaient été jetées au travers de la réunion du G7 à Lyon en 1997, fut adoptée peu de temps après les tragiques événements du 11 septembre, alors que les discussions duraient depuis 3 ans, et que 27 projets de rédaction s'étaient succédés avant de finalement parvenir à un accord. Voir sur ce point : X. Le Cerf, Lutte contre la cybercriminalité : le projet de convention du Conseil de l'Europe sur la cybercriminalité, 19 avril 2001, Juriscom.net, http://www.juriscom.net/pro/2/crim20010419.htm.

[101] dont la France.

[102] La convention, si elle prévoit explicitement la conservation des données de connexion, n'est pas le seul texte supranational dans ce domaine. Dans la même lignée, la directive Vie privée n° 2002-58 du 12 juillet 2002, prise en application de la directive 95-46 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel, qui organise la protection des individus prévoit dans son article 15 une exemption permettant la conservation des traces de connexion : « *1. Les États membres peuvent adopter des mesures législatives visant à limiter la portée des droits et des obligations prévus aux articles 5 et 6, à l'article 8, paragraphes 1, 2, 3 et 4, et à l'article 9 de la présente directive lorsqu'une telle limitation constitue une mesure nécessaire, appropriée et proportionnée, au sein d'une société démocratique, pour sauvegarder la sécurité nationale — c'est-à-dire la sûreté de l'État — la défense et la sécurité publique, ou assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales ou d'utilisations non autorisées du système de communications électroniques, comme le prévoit l'article 13, paragraphe 1, de la directive 95/ 46/CE. À cette fin, les États membres peuvent, entre autres, adopter des mesures législatives prévoyant la conservation de données pendant une durée limitée lorsque cela est justifié par un des motifs énoncés dans le présent paragraphe. Toutes les mesures visées dans le présent paragraphe sont prises dans le respect des principes généraux du droit communautaire, y compris ceux visés à l'article 6, paragraphes 1 et 2, du traité sur l'Union européenne.(...)* »

Article 16 – Conservation rapide de données informatiques stockées

1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour permettre à ses autorités compétentes d'ordonner ou d'imposer d'une autre manière la conservation rapide de données électroniques spécifiées, y compris des données relatives au trafic, stockées au moyen d'un système informatique, notamment lorsqu'il y a des raisons de penser que celles-ci sont particulièrement susceptibles de perte ou de modification.

2. Lorsqu'une Partie fait application du paragraphe 1 ci-dessus, au moyen d'une injonction ordonnant à une personne de conserver des données stockées spécifiées se trouvant en sa possession ou sous son contrôle, cette Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger cette personne à conserver et protéger l'intégrité desdits données pendant une durée aussi longue que nécessaire, jusqu'à maximum 90 jours, afin de permettre aux autorités compétentes d'obtenir leur divulgation. Une Partie peut prévoir qu'une telle injonction soit renouvelée par la suite.

3. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger le gardien des données ou une autre personne chargée de conserver celles-ci à garder le secret sur la mise en œuvre desdites procédures pendant la durée prévue par son droit interne.

Article 20 – Collecte en temps réel des données relatives au trafic

1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à :

a. collecter ou enregistrer par l'application de moyens techniques existant sur son territoire ;

b. obliger un fournisseur de services, dans le cadre de ses capacités techniques existantes, à :

i. collecter ou enregistrer par l'application de moyens techniques existant sur son territoire, ou

ii. prêter aux autorités compétentes son concours et son assistance pour collecter ou enregistrer, en temps réel, les données relatives au trafic associées à des communications spécifiques transmises sur son territoire au moyen d'un système informatique.

On assiste, au fil des évolutions législatives, à un renforcement régulier des mesures imposant la collecte des données de connexion. Il est probable que cette tendance ait vocation à s'intensifier, étendant son domaine à des secteurs non encore directement concernés (comme les réseaux d'entreprise par exemple). En effet, la lutte contre la cybercriminalité implique un contrôle de plus en plus pointu de l'activité des internautes, dans ce contexte les obligations semblant peser uniquement sur les opérateurs de l'internet pourraient à terme être étendues à d'autres acteurs agissant sur le net[103]. Ce type de propos a

[103] En l'état actuel, il existe des cas où la conservation des logs ne peut pas permettre de remonter à l'auteur du comportement fautif. Il en est en tout cas ainsi lorsqu'un réseau interne est connecté à l'internet par le biais d'une passerelle pourvue de la fonction NAT. On peut penser particulièrement aux réseaux d'entreprises mais aussi aux cybercafés ou encore au réseau RENATER (Voir introduction).

d'ailleurs été clairement exprimé, en dehors de nos frontières, par le ministre de l'intérieur britannique, Jack Straw, qui affirmait que *« les données concernant certaines personnes soumises à enquête ne seront disponibles que si les données concernant les communications de l'ensemble de la population sont conservées »*. Même si ces propos peuvent paraître ne pas nous concerner directement, il n'en demeure pas moins qu'ils représentent la tendance actuelle de la législation française.

La lutte contre la criminalité commise au travers des réseaux a pris la forme d'une lutte contre l'anonymat induit par les communications numériques. Pour ce faire il a fallu prendre des mesures en vue d'assurer la traçabilité des communications sur l'internet, ces mesures ne peuvent être efficaces que si l'ensemble des auteurs de chaque échange transitant par le net peut être identifié. Mais tel n'est pas le cas, en effet les connexions effectuées par les réseaux NAT (depuis un intranet d'entreprise par exemple) ne permettent pas, sans certaines données complémentaires[104], de remonter jusqu'à leurs auteurs. Si l'on désire créer une véritable traçabilité alors il faudrait soumettre les réseaux NAT à une obligation de conservation des données de connexion.
Or, en l'état actuel, les textes français posant le principe de conservation des logs, en l'absence de décret d'application, ne permettent pas de déterminer clairement le champ de l'obligation. Plus encore la rédaction de ces mêmes textes pourrait laisser penser que les réseaux d'entreprises connectés à l'internet au travers d'une passerelle équipée de la fonction NAT seraient susceptibles d'être concernés par l'obligation de conservation.

B. Applicabilité des obligations de conservation des données de connexion aux réseaux d'entreprises

L'utilisation de l'informatique est désormais chose commune au sein des entreprises, la mise à disposition d'une connexion à l'internet est, de la même manière, de plus en plus répandue. On estime en effet que trois millions de salariés disposent d'un accès au net depuis leur poste de travail[105].
Le réseau interne des sociétés dispose souvent d'un point de connexion vers l'extérieur (vers l'internet) ; la passerelle utilisée sera généralement un routeur utilisant la fonction NAT, qui rappelons-le, a entre autre pour effet de masquer les ordinateurs de l'entreprise sous l'apparence d'une machine unique (interdisant de ce fait la possibilité de tracer de l'extérieur, les communications émises depuis l'intranet).
En pratique l'officier de police judiciaire qui rechercherait, par exemple, l'auteur d'une incitation à la haine raciale, perpétrée au travers d'une page personnelle mis en ligne sur le net, pourrait ne pas être en mesure de remonter la piste avec les données de connexions conservées par l'hébergeur si celle le mène à un réseau d'entreprise. Il disposera de l'adresse de la société mais celle ci ne permet pas de déterminer le poste émetteur. Comment savoir lequel des deux ou trois milles ordinateurs du réseau de l'entreprise a servi à mettre ce contenu sur l'internet si il ne dispose pas des traces générées par le routeur que seule l'entreprise peut détenir.
Or, comme nous l'avons vu précédemment, il ressort de l'examen des textes imposant la conservation des données de connexion que la nécessité de maintenir la traçabilité des

[104] Il s'agira en fait des logs du routeur.
[105] Voir note de bas de page n° 130.

communications faites sur l'internet représente un besoin en matière de lutte contre la cybercriminalité.
On peut alors se demander si il ne conviendrait pas de soumettre les réseaux d'entreprise aux mêmes obligations de conservation des traces de leur employés afin de ne pas laisser subsister un espace non régulé, offrant un anonymat qui empêcherait toute détermination de l'auteur en cas d'agissements illicites sur le net (2).
Plus encore, on peut être amené à se demander si la rédaction actuelle des textes pourrait, de part son ambiguïté, laisser supposer que l'employeur serait visé par les dispositions législatives, ce point pouvant être éclairé par les développements futurs (mais déjà annoncés) des textes (1).

1. Interprétation et prospective sur la législation imposant la conservation des logs

L'article 43-9 de la loi sur la liberté de communication[106] vise les prestataires mentionnés aux articles 43-7 (personnes offrant un accès) et 43-8 (hébergeurs) leur imposant la conservation des logs des personnes *«ayant contribué à la création d'un contenu des services dont elles sont prestataires ».*

Les articles 43-7 et 43-8, auxquels il est fait référence par le texte, disposent :

> *«article 43-7 : Les personnes physiques ou morales dont l'activité est d'offrir un accès à des services de communication en ligne autres que de correspondance privée sont tenues, d'une part, d'informer leurs abonnés de l'existence de moyens techniques permettant de restreindre l'accès à certains services ou de les sélectionner, d'autre part, de leur proposer au moins un de ces moyens. »*
>
> *« article 43-8 : Les personnes physiques ou morales qui assurent, à titre gratuit ou onéreux, le stockage direct et permanent pour mise à disposition du public de signaux, d'écrits, d'images, de sons ou de messages de toute nature accessibles par ces services, ne sont pénalement ou civilement responsables du fait du contenu de ces services que :*
> *- si, ayant été saisies par une autorité judiciaire, elles n'ont pas agi promptement pour empêcher l'accès à ce contenu ; »*

L'article 43-9 est-il applicable aux entreprises disposant de réseaux ouverts sur l'internet mis à disposition de leurs salariés? On pourrait répondre par la négative objectant que le texte se réfère aux « prestataires » ce qui semble impliquer que ce qui est visé ici est une activité commerciale. Plus encore la phrase : « *conserver les données de nature à permettre l'identification de toute personne ayant contribué à la création d'un contenu des services dont elles sont prestataires »* laisse supposer que ce sont les clients des prestataires et non les employés de l'entreprise qui sont ici concernés[107].

[106] Voir dans ce même chapitre A- 2- Principes énoncés par la loi. p. 29.
[107] Sur ce point voir : V. Sédallian, La responsabilité de l'employeur en tant que fournisseur d'accès à internet, Légicom N° 27-2002/2

Quant à l'article 43-7 auquel il est renvoyé, il concerne les personnes offrant un accès à l'internet. D'un point de vue technique, si l'on considère que la fourniture d'accès consiste à offrir une connexion à l'internet, alors l'entreprise pourrait être assimilée à un FAI en ce qu'elle offre un accès à ses collaborateurs, comme le note Me. Sédaillan : « *Le fournisseur d'accès employeur fournit des accès à ses employés à des fins professionnelles. Il peut avoir un abonnement auprès d'un fournisseur d'accès commercial ou disposer de sa propre infrastructure de connexion à l'Internet* » [108].
Cependant les termes définissant le service de fourniture d'accès paraissent écarter cette assimilation. En effet le texte fait référence aux « abonnés » du fournisseur d'accès, il ne semble pas que les collaborateurs de l'entreprise puissent être qualifiés d'abonnés. En effet, la mise à disposition de la connexion est réalisée à des fins professionnelles et non dans l'optique d'une utilisation personnelle (même si celle-ci est admise en pratique). La connexion ainsi offerte demeure un outil de travail propriété de l'employeur[109], le salarié demeurant tenu par le lien de subordination (caractérisant la relation employeur/employé[110])

> Il faut aussi écarter le cas des connexions offertes à titre privé par certaines grandes entreprises à leurs salariés. Dans ce contexte l'utilisation de la connexion est faite au domicile de l'employé à des fins exclusivement personnelles, en dehors du cadre de travail et de tout contrôle de l'entreprise.

Mais encore l'expression « dont l'activité est de » laisse supposer qu'il s'agit en fait d'une activité principale et non d'une activité accessoire. Or les entreprises, si elles offrent un accès à l'internet, ne le font sûrement pas à titre principal.
Ce qui est donc visé ici est une activité économique et non technique, dans ce contexte il ne semble pas que l'employeur, en tant que fournisseur d'accès de ses employés, puisse être soumis à cette obligation.
Il faut ici noter que, paradoxalement, le futur article 32-3-3 qui devrait être inséré dans le Code des postes et télécommunications par le projet de loi pour la confiance dans l'économie numérique, ne fait aucune référence à l'article 43-7, ou à une quelconque activité économique, pour organiser la responsabilité atténuée des fournisseurs d'accès à l'internet. Le futur article L.32-3-3 du Code des postes et télécommunications prévoit ainsi :

> *« - Toute personne assurant une activité de transmission de contenus sur un réseau de télécommunications ou de fourniture d'accès à un réseau de télécommunications ne peut voir sa responsabilité civile ou pénale engagée à raison de ces contenus que dans les cas où soit elle est à l'origine de la demande de transmission litigieuse, soit elle sélectionne le destinataire de la transmission soit elle sélectionne ou modifie les contenus faisant l'objet de la transmission. »*

[108] V. Sédallian, Droit de l'internet, éditions AUI. Précit. p. 15.
[109] Principe d'ailleurs rappelé par l'arrêt de la Cour d'Appel de Paris, 16 novembre 2001, Bourcy contre SA Expeditors International, qui énonce que l'ordinateur en tant qu' *« outil de travail »* reste la propriété de l'employeur, il lui appartient donc de fixer les conditions de son utilisation.
[110] Voir sur ce point chapitre II. p. 59.

Pourrait-on y voir l'abandon d'une approche « commerciale » de l'activité de fourniture d'accès au profit d'une définition technique[111] ? Si tel était le cas l'entreprise offrant un accès à ses collaborateurs serait plus facilement à même d'être considérée comme un FAI et par là même soumise à l'obligation de conservation des traces.

Par contre l'article 43-8 paraît pouvoir s'appliquer plus aisément aux réseaux d'entreprise, une société peut donc être considérée comme un hébergeur. C'est une activité technique qui est ici décrite, l'employeur qui héberge des contenus mis en ligne sur l'internet (son site e-commerce par exemple) doit donc logiquement être soumis au devoir de conservation des données de connexion des personnes ayant participé à la création de ce contenu.
Par contre si le pages ne sont pas consultables depuis l'internet mais limitées à une diffusion interne à l'entreprise (intranet) l'utilisation des termes : *« pour mise à disposition du public »* pourraient apporter une limitation à l'application de cette disposition. Cependant il convient de noter que la notion de « public » ne recueille pas une acception uniforme. Si en matière de délits de presse[112] un intranet ne peut pas être considéré comme un lieu public en raison de la communauté d'intérêt existant dans l'entreprise ; tel n'est pas le cas en ce qui concerne les droits d'auteur où la communauté d'intérêt n'exclue pas que la diffusion soit entendue comme publique[113].

Pourtant l'évolution législative ne paraît plus aussi formelle, la prochaine réforme de la loi de 1986 diffère par son approche sémantique. Ainsi le projet de loi pour la confiance dans l'économie numérique dispose :

> *« Art. 43-13. - Les personnes mentionnées aux articles 43-7 et 43-8 détiennent et conservent les données de nature à permettre l'identification de quiconque a contribué à la création du contenu ou de l'un des contenus des services dont elles sont prestataires. Elles fournissent aux personnes qui éditent un service de communication publique en ligne des moyens techniques permettant à celles-ci de satisfaire aux conditions d'identification prévues à l'article 43-14.*
>
> *L'autorité judiciaire peut requérir communication auprès des prestataires mentionnés aux articles 43-7 et 43-8 des données mentionnées au premier alinéa.*
> *Les dispositions des articles 226-17, 226-21 et 226-22 du Code pénal sont applicables au traitement de ces données.*

---

[111] D'autant plus que le défunt projet de loi LSI, prédécesseur de la LCEN, faisait, quant à lui, référence à l'article 43-7 dans sa rédaction du texte de l'article 32-3-3. Il prévoyait ainsi : *« Art. L. 32-3-1. - La responsabilité civile d'un opérateur de télécommunications, et notamment d'un prestataire technique exerçant l'activité mentionnée à l'article 43-7 de la loi n° 86-1067 du 30 septembre 1986 relative à la liberté de communication, ne peut être engagée à raison des contenus qu'il se borne à transmettre ».*

[112] Organisé par la loi du 29 juillet 1881.

[113] En dehors d'une décision inspirée par les circonstances de l'affaire. Ord. réf. TGI Paris 10 juin 1997 dit « Queneau » (seconde affaire). JCP 1997, II, 22974, note F. Olivier ; Expertises 1997, p. 283. Le cas concernait *« un réseau privé dédié à la recherche scientifique »* rassemblant plus de 500 personnes, dans lequel avait circulé la contrefaçon d'une œuvre. L'ordonnance constate cependant l'absence de contrefaçon. Mais il convient de noter que cette décision peut être grandement influencée par le cas de l'espèce : l'infraction avait été constatée par un agent assermenté qui s'était introduit, à partir de l'internet, dans un réseau privé sécurisé.

Un décret en Conseil d'Etat, pris après avis de la Commission nationale de l'informatique et des libertés, définit les données mentionnées au premier alinéa et détermine la durée et les modalités de leur conservation. »

On peut noter que le législateur ne se réfère plus ici aux « prestataires » mais aux « personnes » ce qui paraît éliminer un obstacle à l'application du texte aux entreprises[114]. Il reste tout de même encore des points y faisant barrage ; ainsi le texte conserve la référence à la *« création du contenu ou de l'un des contenus des services dont elles sont prestataires »* ce qui comme nous l'avons vu précédemment laisse supposer que ce sont les clients des FAI qui sont visés.
On peut aussi noter que le maintien de la référence à l'article 43-7 semble devoir écarter l'application de ce texte aux réseaux d'entreprise (voir infra p.33).

La loi sur la Sécurité quotidienne[115], instaurant une obligation de conservation des données concernant toute communication, vise quant à elle les *« opérateurs de télécommunications, et notamment ceux mentionnés à l'article 43-7 de la loi no 86-1067 du 30 septembre 1986 »*.
Ici le texte est plus large car il cible les opérateurs de télécommunication dans leur ensemble et particulièrement les fournisseurs d'accès à l'internet. Le recours à l'adverbe « notamment » démontre que la liste n'est pas exhaustive. Ce point suscite quelques interrogations étant donné que le texte assortit le non respect de l'obligation de sanctions pénales, or le droit pénal est gouverné par un principe imposant une interprétation stricte des textes, en opposition avec les imprécisions que l'utilisation de « notamment » fait naître. On peut alors s'interroger sur la position que seront amenées à adopter les juridictions.
Plus encore on peut penser que ce « notamment » n'est pas démonstratif mais inclusif si considère que les activités d'opérateur de télécommunication et de fournisseur d'accès peuvent être différentes, comme le fait l'avis du sénateur Türk sur le projet de loi pour la confiance dans l'économie numérique[116]. Ainsi un câblo-opérateur tel que Noos est un opérateur de télécommunications mais est aussi un fournisseur d'accès et un hébergeur (pour les pages personnelles de ses abonnés) mais toutes ces fonctions restent distinctes. Il ne peut y avoir d'assimilation entre l'activité d'opérateur et celle de FAI ; le « notamment » ajoute donc un cas supplémentaire.

Il convient donc de tenter de définir ce qu'est un opérateur de télécommunication. La définition figure au 15ème alinéa de l'article L 32 du Code des postes et télécommunications :

Article L 32 :

15° Opérateur :
On entend par opérateur toute personne physique ou morale

[114] Ce changement de vocabulaire est fait en contradiction avec la directive sur le commerce électronique du 8 juin 2000 que la LCEN est censée transposer qui, pour sa part, préfère la notion de prestataire à celle de personne.
[115] Voir dans ce même chapitre, A- Un principe général : la conservation et l'accès aux données de connexion. p. 22.
[116] Avis sur le projet de loi pour la confiance dans l'économie numérique. Voir introduction. p. 9.

exploitant un réseau de télécommunications ouvert au public ou fournissant au public un service de télécommunications.

Le même article définit le réseau ouvert au public qu'il faut opposer au réseau indépendant :

3° Réseau ouvert au public.
On entend par réseau ouvert au public tout réseau de télécommunications établi ou utilisé pour la fourniture au public de services de télécommunications.

4° Réseau indépendant.
On entend par réseau indépendant un réseau de télécommunications réservé à un usage privé ou partagé.
Un réseau indépendant est appelé :
- à usage privé, lorsqu'il est réservé à l'usage de la personne physique ou morale qui l'établit ;
- à usage partagé, lorsqu'il est réservé à l'usage de plusieurs personnes physiques ou morales constituées en un ou plusieurs groupes fermés d'utilisateurs, en vue d'échanger des communications internes au sein d'un même groupe.

Les entreprises ne seraient pas des opérateurs de télécommunication, leur réseau n'étant pas normalement ouvert au public, il devrait être qualifié d'indépendant, les salariés de la société formant un groupe fermé d'utilisateurs.

La loi de finance rectificative de l'année 2001 étend, quant à elle, le principe de conservation des logs.
En effet l'article 62 de la LFR vise *« les opérateurs de télécommunications et les prestataires mentionnés aux articles 43-7 et 43-8 de la loi no 86-1067 du 30 septembre 1986 relative à la liberté de communication »*, il semble étendre l'obligation de conservation aux hébergeurs. Or la notion d'hébergeur telle qu'elle transparaît de l'article 43-8 de la loi de 1986 est plus large que celle de FAI, ici il n'y a pas de terme semblant exclure implicitement les entreprises de son champ d'application (pas de référence aux « abonnés » ou à tout autre terme dénotant une activité à caractère commercial).

L'assujettissement des entreprises aux diverses dispositions prévoyant la conservation des données de connexion ne semble pas évidente mais ce point suscite tout de même quelques interrogations. Il est difficile de considérer l'employeur comme un fournisseur d'accès en raison des références faites à une activité commerciale[117].
L'incertitude règne donc en ce domaine et l'absence de décret de transposition ne facilite pas la compréhension de l'économie des textes, comme le note le Forum des droits sur l'internet : *« L'article 29 de la loi sur la sécurité quotidienne du 12 novembre 2001 impose aux opérateurs de télécommunications l'effacement ou l'anonymisation des données de connexion avec deux exceptions liées aux besoins de facturation et aux besoins des enquêtes*

[117] Par contre l'entreprise peut plus facilement être soumise à l'obligation de conservation des traces en raison de sa fonction d'hébergeur (prévue par l'article 43-9 l 86-1067 et LFR 2001).

pénales. Mais, même si ce point mérite explicitement d'être confirmé par les textes, les entreprises ne peuvent être aisément considérées comme des opérateurs de télécommunications au sens des dispositions de cette loi. En effet, elles possèdent des réseaux indépendants qu'elles ouvrent à leurs salariés et non au public. Elles ne seraient donc pas soumises à l'obligation d'effacement ou d'anonymisation des données de connexion.
Ces dispositions nationales devront être rapprochées des stipulations de la convention cybercriminalité du 23 novembre 2001 qui imposent aux Etats d'adopter les mesures nécessaires pour permettre la conservation des données informatiques » [118].
En effet, la convention sur la cybercriminalité semble apporter une réponse plus précise à cette question.
Ainsi celle-ci adopte dans son article 1 c) une définition des fournisseurs de service :

> *« c. «fournisseur de service» désigne :*
> *i. toute entité publique ou privée qui offre aux utilisateurs de ses services la possibilité de communiquer au moyen d'un système informatique ;*
> *ii. toute autre entité traitant ou stockant des données informatiques pour ce service de communication ou ses utilisateurs ; »*

Cette définition des fournisseurs d'accès et des hébergeurs est très large et pourrait tout à fait recouvrir les réseaux d'entreprises. La notion d' « utilisateurs » offre un champ bien plus étendu que celle d' « abonnés » utilisée jusqu'à lors.
D'ailleurs, le rapport final d'activité du Comité d'Experts sur la Criminalité dans le Cyber-espace est très explicite sur ce point en précisant que *« l'expression fournisseur de services englobe de nombreuses catégories de personnes jouant un rôle particulier dans la communication ou le traitement de données sur des systèmes informatiques (…). Au point (i) de la définition, il est précisé que l'expression désigne notamment les entités publiques et privées qui offrent aux utilisateurs la possibilité de communiquer entre eux. Il est donc indifférent que les utilisateurs forment un groupe fermé ou que le fournisseur offre ou non ses services au public, gratuitement ou contre le paiement de droits. Le groupe fermé peut être constitué par les salariés d'une entreprise privée auxquels les services sont fournis par un réseau d'entreprise »* [119].
Il ne s'agit ici que d'un rapport explicatif qui opère une simple interprétation de la convention et non d'un texte à valeur contraignante, mais il permet tout de même de mieux cerner l'étendue des dispositions contenues dans le texte et pourrait servir de guide lors d'une future interprétation jurisprudentielle.

Notons que, pour l'heure, ces définitions adoptées par la convention cybercriminalité ne sont pas d'application directe, elles n'ont pas de conséquence immédiate sur notre droit national. Mais tout cela ne reste vrai que jusqu'à la ratification de la convention. Une fois cette

[118] Forum des droits sur l'internet, Rapport final, Relations de travail et internet, adopté le 17 septembre 2002, note 36, http://www.foruminternet.org/publications/lire.phtml?id=396.
[119] Rapport final d'activité adopté par le Comité européen pour les problèmes criminels (CDPC) lors de sa 50ème session plénière (18-22 juin 2001). (Dernière phrase soulignée par nos soins).

démarche accomplie ces dispositions, ayant valeur de traité, auront une valeur supérieure à celle des lois et règlements[120] .
La conséquence en sera vraisemblablement une extension du champ des personnes soumises à l'obligation de conservation des données de connexion. En effet, dès ratification, ces dispositions prévaudront sur nos règles nationales (LSQ, LFR, Loi de 1986,…), il en découlerait, en respectant la volonté des rédacteurs de ce texte, que les entreprises seraient logiquement soumises au devoir de conservation des logs. Il faut en effet noter que l'ensemble des dispositions créant une obligation de conservation des traces de connexion font référence, pour définir leur champ d'application, aux seules définitions légales des prestataires de l'internet contenues aux articles 43-7 et 43-8 de la loi de 1986. Si les définitions issues de la convention cybercriminalité devaient, à terme, remplacer celles jusqu'à lors utilisées, les réseaux d'entreprise se verraient alors directement intégrés dans le champ des articles 43-9 (futur 43-13) de la loi de 1986, 33-2-1 du Code des postes et télécommunications (inséré par la LSQ) et 60-1 du Code procédure pénale (inséré par la LSI).

La convention, qui avait été signée dès l'origine par la France, n'a depuis jamais été ratifiée. Cependant les choses sont en train d'évoluer. En effet au cours du Conseil des ministres du mercredi 11 juin 2003, Dominique de Villepin, ministre des Affaires Etrangères, a présenté un projet de loi autorisant l'approbation par la France de la convention[121].
L'entrée en vigueur du traité nécessite 5 ratifications, pour l'instant seuls 3 états l'ont ratifié[122], la France sera le quatrième.
Cette convention, qui a pour vocation l'unification des législations en matière de répression de la criminalité informatique, aura le mérite d'éclaircir une situation troublée par l'ambiguïté de la rédaction des textes et le mutisme conservé par le gouvernement concernant les décrets d'application tant de la loi de 1986 que de la LSQ.

Si cet éclaircissement pourrait encore provoquer quelques réticences des autorités en charge de la protection des données à caractère personnel, en raison de la limitation des libertés individuelles qu'il induit (extension du champ d'application de la conservation des données de connexion), il est tout de même salutaire du point de vue de la sécurité juridique.

Au delà des textes, et des interrogations qu'ils peuvent susciter, la conservation logs peut trouver une justification dans des considérations d'ordre pratique. La nécessité de conserver les traces de connexion ne devrait pas, en toute logique, être écartée dans le cas des réseaux NAT, dans le cas contraire, il en résulterait la reconnaissance de l'existence d'un espace non régulé, placé hors du droit.

2. Arguments d'ordre pratique

Comme nous avons pu le voir précédemment, les acteurs de l'internet sont soumis à une obligation de conservation des données de connexion pour une raison simple, celle-ci tenant

[120] En vertu de la hiérarchie des normes. Le traité a une valeur supérieure aux dispositions d'ordre national même sur la constitution (H. Kelsen).
[121] Actualités, Cybercriminalité : un projet de loi pour adapter le droit. Disponible sur le site http://www.premier-ministre.gouv.fr.
[122] A savoir l'Albanie (20-06-02), la Croatie (17-10-02) et l'Estonie (12-05-03).

au fait qu'ils sont les seuls à pouvoir permettre l'identification d'un auteur d'un comportement illicite sur l'internet. Or la détermination des auteurs d'actes illicites est devenue une préoccupation majeure des autorités judiciaires.
La lutte contre l'anonymat que l'internet pouvait faire naître était une tâche primordiale. Mais en réalité l'anonymat sur le net n'est qu'apparent et en fait chaque connexion est en fait aisément traçable. Du moins tel est généralement le cas, car la traçabilité, inhérente au protocole utilisé sur l'internet[123], peut être rompue. Il peut en être ainsi, notamment, lorsque qu'un réseau local (un intranet par exemple) est relié à l'internet au moyen d'un routeur pourvu de la fonctionnalité NAT. Dans cette situation particulière, les forces de l'ordre pourraient être dans l'incapacité de retrouver l'auteur d'une infraction commise à partir d'un réseau d'entreprise
Ainsi que cela a été exposé précédemment[124] le NAT peut avoir pour effet de masquer totalement les ordinateurs de l'entreprise reliés à l'internet (qui apparaîtront comme une machine unique). L'opérateur de télécommunications au travers des logs qu'il aura conservé, ne sera pas en mesure de déterminer quelle machine (quel poste du réseau de l'entreprise[125]) a été à l'origine des actes frauduleux. Dans ce cas *« le lien avec une personne déterminée n'est pas toujours évident. En effet, dans le cadre d'une connexion à partir d'un réseau d'entreprise ou d'un cybercafé, il sera difficile de déterminer avec certitude l'identité de l'internaute »*[126].
L'entreprise qui a loué les lignes de télécommunication a, ici, un rôle semblable à celui d'un fournisseur d'accès internet[127]. Vu de l'extérieur tout se passe comme si le réseau local n'était qu'une seule et unique machine. L'adresse IP retrouvée sera celle du routeur NAT[128] et non les adresses privées, dont chaque ordinateur du réseau est pourvu, et qui permettraient de l'identifier précisément si elles étaient visibles de l'extérieur.
Ce sont donc potentiellement des centaines, voire des milliers d'ordinateurs[129] et donc d'utilisateurs qui sont ainsi soustraits à toute possibilité d'identification. En effet, *« on estime qu'environ 20 % des salariés français, soit approximativement trois millions de personnes, disposent d'un accès à Internet »*.[130]
Alors que l'évolution législative tend à assurer de plus en plus la traçabilité, la translation d'adresses peut y apporter une limite importante en remettant en cause l'édifice législatif.

Les arguments pratiques qui ont été avancés afin de justifier la conservation des données de connexion par les prestataires de l'internet peuvent être repris ici dans les mêmes termes. La possibilité de retracer les origines des connexions n'est envisageable qu'avec les informations contenues dans les fichiers logs du routeur (ou de la passerelle quelle qu'elle soit) NAT, sans eux la traçabilité peut être définitivement et irrémédiablement rompue.

---

[123] Liée à l'adressage IP notamment. Voir introduction pour de plus amples développements.
[124] Voir développements relatifs au NAT dans l'introduction.
[125] Le raisonnement est aussi valable dans le cas d'un utilisateur connecté depuis un cybercafé, une administration ou encore au travers du réseau universitaire RENATER.
[126] P. Belloir, e-délinquance, Legalis.net, 2002-2, p.24.
[127] Voir la distinction des fonctions dans l'avis du sénateur Türk. Précit.
[128] C'est-à-dire la seule IP dite « routable ».
[129] Les réseaux des grands groupes du CAC 40, en raison de leurs grands besoins en système d'information, comprennent plusieurs milliers de stations en réseau (elle servent parfois de fournisseur d'accès pour leurs sous-traitants) souvent avec un ou deux points d'accès à très haut débit les reliant à l'internet.
[130] Réponse à la question du sénateur Trégouët (Question écrite Nº 07822 du 05/06/2003 page 1777 avec réponse posée par TRÉGOUËT (René) du groupe UMP)**.** Ministère de réponse: Affaires sociales - Publiée dans le JO Sénat du 24/07/2003 page 2370**.**

Un exemple des infractions pouvant être commises par le biais de la connexion à l'internet fournie par l'employeur : le *peer to peer*.

Les infractions pouvant être commises au travers des réseaux d'entreprise sont variées, le cas le plus fréquent reste sans doute le téléchargement de fichiers musicaux en contravention des droits d'auteur. Ces dernières années on vu proliférer le partage de fichiers, au travers d'un système baptisé *« Peer to peer »*[131] (ou liaison point à point, P2P). Ces échanges sont le plus souvent faits en contravention des droits d'auteur et sont pénalement punissables par le Code de la propriété intellectuelle.

On a ainsi constaté que les réseaux d'entreprise étaient fréquemment utilisés par les employés afin de « pirater » des œuvres protégées. « *Le Peer-to-Peer aurait contaminé trois entreprises sur quatre, selon une étude réalisée par AssetMetric, société canadienne spécialisée dans l'audit de systèmes informatiques. L'étude révèle que 77 % des entreprises interrogées possèdent au moins un ordinateur sur lequel est installé un programme comme KaZaa, Imesh ou Edonkey.*
En moyenne, les plus petites structures enregistrent un taux moyen d'utilisation de programme P2P de 8% (contre 2% pour les sociétés de plus de 500 employés). Selon l'étude, ce taux varie en fonction de la taille des sociétés et des mesures mises en place pour contrer le réseau d'échange. Ainsi, 10% du parc informatique des grandes sociétés est concerné, contre 20 à 30% pour les plus petites. »[132]

Le fait est que, dans la pratique, les connexions illimitées à haut débit (comme l'ADSL) ne sont pas encore légion dans les foyers français (même si des efforts ont été effectués pour permettre le déploiement de ce type de technologie). A l'opposé, les entreprises disposent souvent de connexions à l'internet avec une bande passante importante.
Quand on sait que le téléchargement de fichiers musicaux, de films ou autres progiciels peut représenter plusieurs heures de connexion, on comprend bien que mieux vaut disposer d'une liaison rapide et illimitée à l'internet et donc de s'adonner à ces pratiques au bureau.

Or l'engouement qu'a suscité le partage de fichiers par l'internet a provoqué une forte réaction des maisons de disque principalement.
Les poursuites contre des utilisateurs acharnés n'en sont qu'à leur début[133], les éditeurs, associés dans la lutte contre le piratage[134], n'ont de cesse de demander aux fournisseurs d'accès d'identifier les abonnés mis en cause dans ce type de pratique.
Conjointement les maisons de disque ont mis en garde les entreprises contre le piratage d'œuvre protégées qui avait lieu au travers de leurs infrastructures réseau. Ainsi le RIAA (*Recording Industry Association of America*), aux Etats Unis, a envoyé des lettres mettant en demeure ces sociétés de prendre les mesures adéquates afin de faire cesser ces infractions[135].

---

[131] Voir glossaire des termes techniques en annexe.
[132] Le Monde Informatique, 17 juillet 2003, Le peer to peer envahit trois entreprises sur quatre.
[133] Les poursuites ne font que commencer notamment aux USA où le RIAA (*Recording Industry Association of America*) vient d'obtenir 871 ordonnances fédérales enjoignant à des prestataires techniques de lui communiquer les coordonnées de personnes suspectées d'avoir échangé sur l'Internet de nombreuses œuvres contrefaisantes, mais déjà sont dans sa ligne de mire l'Italie et l'Espagne.
[134] Notamment aux Etats Unis le RIAA (*Recording Industry Association of America).*
[135] Reuters, 17 mars 2003, *Music group sends piracy complaints to 300 firms.*

Le cas n'est pas isolé, les cybercafés ont aussi été la cible des foudres de l'industrie musicale. La chaîne de cybercafés Easy Internet a du parvenir à un accord pour ne pas risquer de poursuite pour avoir facilité le piratage de morceaux musicaux par l'internet[136].
Un peu plus tard se devait être au tour des réseaux des universités américaines d'être visés par le courroux des maisons de disque[137].

> Il faut souligner que l'important lobby que représente l'industrie musicale pourrait, si le besoin s'en fait sentir, tenter de faire adopter des mesures afin de permettre une traçabilité accrue sur l'internet (sur le réseaux d'entreprises pourquoi pas ?). Le RIAA a déjà fait une démonstration de force en amenant les sénateurs américains a examiner un amendement permettant aux auteurs de se faire justice eux mêmes en cas de piratage de leurs œuvres (par des systèmes d'autodestruction notamment)[138].

Le fait que les maisons de disque s'adressent aux entreprises et non directement à leurs employés est motivé par leur incapacité à remonter jusqu'à l'auteur de l'infraction.
Si l'entreprise d'où émane la communication est aisément identifiable par l'adresse IP externe de la passerelle, il est impossible de remonter plus en amont vers le poste à l'origine de la connexion et ce en raison de la translation d'adresse. Seule la société est en mesure de restaurer la traçabilité si elle dispose des logs du routeur NAT.

L'éventualité d'une utilisation de la connexion à l'internet fournie par l'employeur dans une intention frauduleuse et répréhensible correspond à une réalité pratique. L'exemple du *peer to peer*, s'il est sans doute le plus fréquent, n'est cependant pas le seul, l'utilisation des moyens offerts au salarié peuvent aussi permettre d'autres comportements fautifs tels les diffamations[139], le hacking[140] l'envoi de virus, le téléchargement et la distribution d'images à caractère pédophile[141], l'incitation à la haine raciale ou encore des menaces terroristes.

Alors que les lois adoptées en matière de conservation des données de connexion n'ont pas hésité à apporter des limitations aux libertés individuelles et au principe de respect de la vie privée[142], on peut difficilement admettre que certains secteurs (comme les réseaux NAT) soient exemptés de toute régulation.

La législation française établissant à la charge des acteurs du net une obligation de conservation des données de connexion reste souvent assez ambiguë, mais comme on a pu le

---

[136] Zdnet, 10 avril 2003, Easy Internet règle son différent avec les maisons de disque.
Forum des droits sur l'internet, 10 avril 2003, actualités, Musique en ligne : les cybercafés britanniques payent la note.
[137] Forum des droits sur l'internet, 8 avril 2003, L'industrie musicale américaine s'attaque aux réseaux locaux universitaires.
[138] Les Petites Affiches, Etats Unis- Réseaux P2P : l'industrie américaine du disque pourra-t-elle se faire justice elle-même ? 28 janvier 2003.
[139] Dont un exemple récent nous est fourni par l'affaire ESCOTA. Voir infra II.
[140] Voir glossaire des termes techniques en annexe.
[141] Il semblerait, aux dires de certains administrateurs réseau de grandes entreprises, que ce genre de « pratiques » ne soient aussi rares que l'on aurait pu le supposer.
[142] Pourtant hautement défendue par la convention de sauvegarde des droits de l'homme et l'article 9 du Code civil. De même la Déclaration universelle des droits de l'homme du 10 décembre 1948 dispose en son article 12 : « Nul ne fera l'objet d'immixtions arbitraires dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteinte à son honneur ou à sa réputation. »

remarquer, au travers de l'évolution des textes depuis quelques années, la tendance est à une généralisation des mesures permettant de retracer les communications.
Les développements attendus devraient encore confirmer cette tendance. Dans ce contexte les entreprises seront peut-être bientôt être amenées à conserver les logs des connexions de leurs employés. Il est évident que la charge financière que cela entraînera sera conséquente (espace de stockage/ possibilité d'accès aux données).
Ironiquement la LSQ prévoit qu'il appartient à l'Etat de dédommager les personnes soumises à cette obligation, cependant ce dédommagement n'a sans doute pas été prévu à l'origine pour les grandes entreprises. Il paraît d'ailleurs peu réaliste que les sociétés du CAC 40 reçoivent une compensation financière en contrepartie de leur assujettissement au devoir de conservation des logs. Quoi qu'il en soit, le décret prévoyant les modalités de ce support financier se fait encore attendre.
Notons enfin qu'en pratique, il y a eu à notre connaissance au moins une demande de communication des données de connexion d'un salarié d'une entreprise du CAC 40 par les autorités judiciaires. Demande effectuée au début de l'année 2003 et couronnée de succès, l'entreprise s'étant exécutée. Mais en avait-elle le droit vis à vis des engagements qu'elle avait pris envers ses salariés ou la CNIL ? Car en effet, si les libertés de l'internaute-citoyen ont pu facilement être limitées, celles du salarié-internaute n'ont de cesse d'être réaffirmées et protégées. La réelle difficulté que pourraient alors connaître les entreprises en matière de conservation des logs pourrait venir de la confrontation entre le devoir d'assurer la traçabilité et les développements jurisprudentiels relayés par certaines autorités garantissant le respect de la vie privée au salarié dans le cadre de son travail.

L'obligation de conservation des données de connexion tient une place primordiale dans lutte contre la cybercriminalité, l'enjeu qu'elle constitue risque de susciter de nombreux débats dans l'avenir.

Chapitre II – L'entreprise à l'heure de l'internet : conservation des traces et responsabilité

Les architectures informatiques mises en place dans les sociétés peuvent faire apparaître l'employeur comme un véritable fournisseur d'accès, qui pourrait ainsi être soumis au devoir de conservation des données de connexion. Or cette obligation, appliquée dans le cadre de l'entreprise, fait naître de nouvelles difficultés. Comment concilier le régime juridique propre aux prestataires de l'internet avec les dispositions particulières, issues notamment du droit social, applicables dans le monde du travail ?

En effet, l'employeur est susceptible de fournir une connexion à l'internet à ses collaborateurs pour faciliter leur travail. Cette mise à disposition s'explique par les économies de temps et d'argent que peut permettre l'ordinateur. Cependant, face aux tendances intrusives que peuvent représenter les nouvelles technologies, s'est affirmé un « droit » pour le salarié à détourner son outil de travail à des fins personnelles[143]. Les différents rapports rendus sur le thème de la cybersurveillance des salariés estiment qu'*« il serait irréaliste de priver les salariés de tout usage personnel des moyens informatiques mis à leur disposition par l'entreprise ... »*[144]. Cet état de fait est relayé par le sentiment qu'entretiennent les salariés qui ont tendance à penser « *que cette utilisation personnelle doit être acceptée par l'employeur. Elle n'est d'ailleurs souvent que la contrepartie de l'interpénétration entre vie personnelle et vie professionnelle. Si leur employeur peut empiéter sur leur vie personnelle, par exemple en leur confiant des ordinateurs portables pour pouvoir assurer leur activité de manière nomade ou en les joignant sur leur téléphone portable, il apparaît logique qu'ils puissent utiliser internet à des fins personnelles sur le lieu de travail.*

Certains vont jusqu'à considérer que cette utilisation est un droit que doit leur assurer l'employeur. Pour ces salariés, l'entreprise devrait favoriser l'existence d'une sphère personnelle au bureau et donc permettre à tous les salariés d'avoir un accès aux technologies de l'information »[145].

Ce dernier point de vue a été repris par certains auteurs qui ont pu ainsi affirmer que *« l'employeur ne peut interdire l'emploi non professionnel de l'ordinateur »*[146].

---

[143] Le gain de productivité recherché au travers de l'informatisation peut être grandement mis à mal par la possibilité d'évasion que peut procurer l'internet comme le notait le sénateur Trégouët : *« M. René Trégouët attire l'attention de M. le ministre des affaires sociales, du travail et de la solidarité sur l'apparition d'un problème assez récent dans les entreprises né de la montée en puissance de l'utilisation d'internet. En effet, un nombre toujours plus important de salariés se trouvent connectés au temps et au lieu de travail, ce qui en incite beaucoup à y passer un temps conséquent qu'ils ne consacrent plus forcément à leurs obligations contractuelles. Les employeurs se trouvent donc de plus en plus souvent confrontés à une situation de diminution de la productivité alors que la surveillance nécessaire pour détecter tout abus s'avère délicate voire coûteuse. »* Question écrite N° 07822 du 05/06/2003 p. 1777, avec réponse posée par R. Trégouët du groupe UMP lors du débat concernant le projet de loi pour la confiance dans l'économie numérique.

[144] CNIL, 23ème rapport d'activité 2002, p.17.

[145] Forum des droits sur l'internet, Rapport final relations de travail et internet, p. 12, http://www.foruminternet.org/publications/lire.phtml?id=396.

[146] G. Lyon-Caen, Sem. Soc. Lamy, n°1046. Suite à l'arrêt « Nikon ». Le fondement de « l'interdiction d'interdire » serait l'article 122-35 du Code du travail qui dispose *« nul ne peut apporter aux droit des personnes et aux libertés individuelles et collectives des restrictions qui ne seraient pas justifiées par la nature de la tâche à accomplir ni proportionnés au but recherché »*. Il semblerait, dans ce contexte, que l'accès à l'internet soit érigé en liberté devant être défendue contre toute atteinte, ce qui paraît être une interprétation extrêmement extensive du texte. Le droit à la connexion deviendrait-il un droit inaliénable de l'individu ?

Il n'est pas évident qu'il existe un droit absolu à l'utilisation non professionnelle de la connexion offerte par l'employeur, au contraire les décisions jurisprudentielles ont affirmé la propriété de l'entreprise sur les matériels mis à la disposition des collaborateurs, ceux-ci devant être utilisés selon les directives du chef d'entreprise[147].

Ce point a une importance non négligeable car les moyens offerts aux salariés permettent une communication quasi instantanée, notamment via les messageries électroniques. Les conséquences d'un acte commis sur le réseau peuvent être incommensurables, en effet un message diffamant par exemple, pourra en un laps de temps très bref, être copié et retransmis pour faire le tour de la planète en quelques jours, voire quelques heures. L'entreprise doit donc prendre en compte ces nouveaux développements induits par les technologies de l'information et de la communication. En effet, le risque reste très présent pour les sociétés offrant un accès à l'internet à leurs collaborateurs, car si les prestataires du net (FAI ou hébergeurs) ont vu leurs responsabilités limitées dans le cadre de leur fonction technique (en contrepartie de la conservation des traces), l'entreprise quant à elle ne bénéficie pas de ce régime : elle reste civilement responsable des actes commis par ses préposés dans le cadre de leurs fonctions[148].

On assiste donc à une affirmation de l'existence d'une vie privée au travail sur laquelle l'entreprise ne peut empiéter, ce qui pourrait être un obstacle à la conservation, par l'employeur, des traces de connexion de ses employés (B). La reconnaissance d'une sphère de liberté à l'employé n'est pas sans conséquences pour l'entreprise, celle-ci est en effet susceptible de voir sa responsabilité engagée du fait des actes commis par ses collaborateurs, notamment en ce qui concerne l'utilisation de l'internet (A).

A. La responsabilité de l'entreprise dans le cadre de la fourniture d'accès à l'internet

L'employé disposant d'une connexion fournie par sa société se voit donc reconnaître une sorte de « droit » à une utilisation non professionnelle de l'outil informatique mis à sa disposition. En termes de responsabilité, on peut comprendre que l'employeur soit réticent à autoriser toute utilisation étrangère au service, en effet étant donné l'importance des conséquences que peut avoir tout propos tenu sur l'internet, en raison de la vitesse et de la volatilité des informations, il pourrait être tenu responsable d'actes commis, depuis leur poste de travail, par ses préposés en dehors de leurs fonctions.
L'entreprise qui offre une connexion à ses employés, agissant à la manière d'un fournisseur d'accès internet, peut craindre que sa responsabilité civile (1), voire sa responsabilité pénale soit mise en jeu (2). L'admission d'un usage non professionnel de la connexion à l'internet ne lui permet plus de maîtriser les risques qu'elle peut être amenée à assumer.

1. La responsabilité civile de l'employeur

La responsabilité civile de l'employeur répond à un régime spécial, prévu par l'article 1384 alinéa 5 du Code civil organisant la responsabilité du commettant pour les actes de ses préposés ; on peut être amené à s'interroger sur l'opportunité d'une application d'un tel texte

[147] Cour d'Appel de Paris, 16 novembre 2001, Bourcy contre SA Expeditors International.
[148] Principe entendu largement par la jurisprudence.

qui reviendrait à rechercher la responsabilité de l'employeur pour des actes commis par ses employés à l'occasion de l'utilisation de l'internet même étrangère au service, et ce, alors que celui-ci se voit quasiment contraint d'autoriser un usage non professionnel de la connexion mise à disposition de ses salariés. Dans ce cas ne conviendrait-il pas de prévoir un régime allégé de responsabilité comme celui des fournisseurs d'accès internet ? (b). Les développements jurisprudentiels récents ne vont pas en ce sens (a).

a) L'employeur fournisseur d'accès reste soumis à 1384 al.5

L'article 1384 alinéa 5 prévoyant la responsabilité du commettant pour les actes de ses préposés dispose que : « *les maîtres et les commettants [sont responsables] du dommage causé par leurs domestiques et préposés dans les fonctions auxquelles ils les ont employés*. »
Une jurisprudence récente est venue affirmer la responsabilité de l'employeur en raison des actes commis par un de ses salariés au travers de la connexion internet fournie par l'entreprise[149].
En l'espèce un salarié de la société Lucent Technologies, mécontent des prix pratiqués par une société d'autoroute (Escota) avait mis en ligne, depuis son poste de travail, un site reproduisant, en les détourant, les pages du site escota.com. Le contenu ainsi créé était hébergé sur les pages personnelles de l'employé chez Multimania.
Escota obtint, par une ordonnance de référé en date du 4 août 2000, la suspension du site auprès de Multimania et la transmission par cette dernière des données de connexion permettant l'identification du créateur des pages incriminées. L'analyse de ces traces permit de remonter jusqu'à la société Lucent Technologies.
La société d'autoroute décida d'agir en justice contre l'auteur mais aussi contre l'hébergeur et l'employeur.
Si la mise en cause de la responsabilité de l'auteur ne fait aucun doute, le tribunal retient aussi celle de l'entreprise sur le fondement de l'article 1384 alinéa 5 du Code civil.
Il était ainsi reproché à l'entreprise d'avoir autorisé ses salariés à utiliser les équipements informatiques mis à leur disposition ainsi que la connexion à l'internet pour des besoins n'ayant pas de relations directe avec leur activité professionnelle[150]. Le tribunal relève donc *« qu'aucune interdiction spécifique (...) quant à l'éventuelle réalisation de sites internet ou de fourniture d'informations sur des pages personnelles »* pour en déduire que la faute du salarié *« a été commise dans le cadre des fonctions auxquelles il était employé ».*
En conséquence l'employeur se voit condamné *in solidum* avec son employé à prendre en charge les frais liés à la procédure.
L'admission de la responsabilité civile de l'entreprise en raison des actes de ses préposés sur le net aux seuls motifs qu'elle n'a pas interdit toute utilisation de l'outil informatique pour des besoins étrangers au service, créé un risque important pour les entreprises. Cela est encore plus vrai dans le cadre de la décision Escota, en effet, dans le cas de l'espèce, il existait une interdiction faite à un usage illicite du réseau, le tribunal relève en effet que *« une*

---

[149] TGI Marseille, Première chambre civile, 11 juin 2003, Escota contre Lucent Technologies, , Juriscom.net, http://www.juriscom.net/jpt/visu.php?ID=273 ; L. Thoumyre, Affaire ESCOTA : un employeur jugé responsable d'un site litigieux réalisé par son salarié , Juriscom.net, actualités, http://www.juriscom.net/actu/visu.php?ID=274. Noter que cette reste contestée par nombre de commentateurs (notamment M. F. Le Tallec). Voir http://www.01net.com/article/212915.html ou encore http://www.afjv.com/juridique/030725_social.html.

[150] Comme le recommandent d'ailleurs généralement les organismes ayant eu à se pencher sur la cybersurveillance des salariés (dont la CNIL et le FDI).

note du directeur des ressources humaines (...) précise que les salariés peuvent désormais utiliser les équipements informatiques mis à leur disposition et les accès réseau existants pour consulter d'autre sites que ceux présentant un intérêt en relation directe avec leur activité(...) dès lors que ces utilisations demeurent raisonnables (...) et respectent les dispositions légales régissant ce type de communication (...), l'accès au sites à caractère explicitement sexuel et contrevenant aux valeurs de Lucent étant prohibé ». Pour le tribunal, cette note ne constitue pas une interdiction spécifique de l'utilisation de la connexion pour la réalisation et la mise en ligne de sites.
Il est donc en fait reproché à l'employeur de ne pas avoir établit une liste exhaustive de tous les comportements interdits. Il faut donc admettre, si cette jurisprudence venait à être confirmée, que les règlements intérieurs, auxquels sont normalement annexées les chartes prévoyant l'utilisation de l'internet[151], devraient prévoir de manière très précise les usages prohibés de la connexion fournie par l'employeur.
La jurisprudence, dans cette affaire, a entendu soumettre l'employeur à un régime de responsabilité stricte en faisant une application large de l'article 1384 al. 5 du Code civil. Cette extension est réalisée aux motifs que les interdictions formulées par l'employeur laissaient place à une utilisation non professionnelle des matériels et de la connexion. L'employeur qui, conformément aux recommandations de CNIL, a autorisé un usage privé de l'outil de travail se voit ainsi sanctionné.
La société peut donc *« voir sa responsabilité engagée pour une utilisation illicite ou fautive d'internet sur le lieu de travail. En effet, civilement, l'employeur est responsable, en tant que commettant de ses salariés, des fautes commises par ceux-ci dans leur utilisation d'internet pendant le temps de travail, sur le fondement de l'article 1384 alinéa 5 du Code civil ».* Cependant normalement*, « l'employeur peut s'exonérer de sa responsabilité si son préposé agit hors des fonctions auxquelles il est employé, sans autorisation et à des fins étrangères à ses attributions. Toutefois, sa responsabilité peut être largement recherchée. Sa vigilance s'impose donc »*[152].

Il est vrai que la jurisprudence, dans d'autres domaines, avait eu tendance a faire une application large de la responsabilité du commettant en considérant que, dès le moment que le salarié a agit sur son lieu de travail pendant le temps et à l'occasion de celui-ci, l'employé n'agissait pas en dehors de ses fonctions. Alors que normalement la responsabilité du commettant ne peut être mise en cause lorsque le préposé a agi à des fins étrangères à ses attributions, c'est-à-dire à l'intérêt du commettant, sans l'autorisation de celui-ci et qu'il s'est placé hors de ses fonctions[153], ces trois conditions étant cumulatives.
Cependant il a été admis, au niveau pénal, que la responsabilité de l'employeur pouvait être reconnue dès lors que l'employé a agit dans le cadre de ses fonctions[154]. Il suffit que l'activité professionnelle ait facilité la commission de l'acte fautif. Cette position s'explique par une volonté de protection de la victime, l'employeur étant normalement solvable, il

[151] Les chartes sont en général annexées au règlement intérieur de l'entreprise pour leur conférer une valeur contraignante. Il faut alors qu'elles respectent la procédure propre à l'adoption du règlement intérieur (avis du comité d'entreprise, transmission à l'inspecteur du travail, publicité). Voir sur ce point, FDI, rapport final, relations de travail et internet. p. 19. précit.
[152] Forum des droits sur l'internet, Rapport final, Relation de travail et internet, 17 septembre 2002. p. 13.
[153] Cour de cassation, Ass. Plen., 19 mai 1988.
[154] Cour de cassation, Ch. Crim., 25 mars 1998. En l'espèce un salarié avait tué son supérieur hiérarchique. L'employeur est déclaré civilement responsable car le crime a été commis sur le lieu de travail et à l'occasion des fonctions exercées par le salarié

constitue une garantie de l'indemnisation des tiers. Il faut tout de même noter que, dans ce contexte, l'entreprise conserve des recours contre son salarié fautif (mais souvent insolvable). Mais, jusqu'à lors, la jurisprudence n'avait pas admis la responsabilité de l'employeur du seul fait de l'utilisation du matériel professionnel par le salarié. Dans une affaire similaire, le TGI de Lyon[155] avait écarté la mise en cause de la responsabilité de l'employeur sur le fondement de l'article 1384 alinéa 5 aux motifs que l'employé (qui s'était servi de l'ordinateur et de la connexion mise à sa disposition pour saturer le serveur de l'entreprise qui l'avait précédemment licencié) *« a agi à l'insu de son employeur - lequel le licenciera, dans la foulée - et que les actes qu'il a commis sont, sans contestation possible, étrangers à l'exercice de ses fonctions : c'est bien en détournant l'usage du matériel qui lui était attribué, que C. a réussi à saturer la bande passante de la société Claranet. »*

Cette responsabilité étendue de l'employeur qui fournit un accès à l'internet à ses salariés engendre un risque important pour l'entreprise bien loin du principe d'irresponsabilité reconnu aux fournisseurs d'accès commerciaux[156].

b) La responsabilité de l'entreprise face à celle du FAI

L'employeur, en tant qu'il offre une connexion à l'internet à ses salariés, se voit donc imposer un régime de responsabilité stricte, mal adapté aux possibilités offertes aux salariés par les nouvelles technologies. Ceci est encore renforcé par l'affirmation sans cesse plus présente d'un droit à la vie personnelle au sein de l'entreprise[157].

Alors que la jurisprudence semble vouloir étendre la responsabilité du commettant, le projet de loi pour la confiance dans l'économie numérique organise une limitation de responsabilité étendue [n'oublions pas l'article 43-12 qui fera obligation aux FAI de filter sur ordre du juge !, il n'y a donc pas une totale irresponsabilité] des FAI (pour leurs activités de fourniture d'accès en tant que telles et pour le service de proxy).
Le principe sous-tendu est celui de l'irresponsabilité des fournisseurs d'accès[158]. L'entreprise pourra-t-elle bénéficier de ce régime de responsabilité allégée ? Cela reste difficilement envisageable, même si la rédaction du texte laisse la place à une application large n'excluant pas expressément les réseaux d'entreprise[159], on ne peut que constater les logiques antinomiques opposant les deux régimes de responsabilité (fournisseur d'accès et commettant), alors que d'un coté le législateur organise une quasi-irresponsabilité des FAI, de l'autre la jurisprudence étend, de plus en plus largement, le champ de la responsabilité des commettants du fait de leurs préposés.

La conservation des traces des connexions des salariés ne pourrait, dans le cas de l'entreprise, conduire à lui appliquer le principe d'irresponsabilité. En effet, la tendance de la jurisprudence à admettre la responsabilité de l'employeur en raison des actes de ses préposés

[155] TGI Lyon, Claranet c/ P. Combe, 20 février 2001.
[156] Selon la distinction faite par Me V. Sédallian dans son ouvrage « Droit de l'internet », précit. p.12.
[157] Voir dans ce même chapitre B. p. 69.
[158] Il est complété par un article 32-3-4 (transposant l'article 13 de la directive) en ce qui concerne les activités de proxy.
[159] Il n'est pas fait référence à l'article 43-7 (qui sert de définition légale des FAI) ni aux opérateurs de télécommunications. Voir infra pour de plus amples développements sur ce point, chapitre I, p.34.

a été réalisée par faveur envers les victimes (pour des raisons liées au manque de solvabilité du salarié[160]). La décision Escota (même si elle reste contestable sur certains points), ne semble pas vouloir infirmer l'édifice jurisprudentiel, bien au contraire elle renforce encore un peu plus la possibilité de mise en cause de la responsabilité de l'entreprise. Cette construction jurisprudentielle, si elle peut être adaptée aux situations courantes rencontrées dans la vie de l'entreprise, parait par contre inadéquate dans le cas de la fourniture par l'employeur d'une connexion à l'internet. Comme nous l'avons vu précédemment, la liberté laissée aux salariés dans leur utilisation de l'outil informatique, conjointement avec les répercussions que peut avoir la diffusion sur le net (importance des dommages causés), laisse place à une très large possibilité d'engagement de la responsabilité de l'employeur sur des actes qu'il ne peut contrôler totalement.

Le raisonnement ici adopté pour la responsabilité civile est-il transposable à la responsabilité pénale de l'employeur ?

2. La responsabilité pénale de l'employeur en tant que fournisseur d'accès

Le principe de responsabilité pour autrui admis en matière civile semble difficilement reproductible au plan pénal, cela tenant au fait que la responsabilité des personnes morales, si elle est prévue par les textes, est limitée au cas où l'infraction a été commise par un organe ou un représentant de la personne morale et pour le compte de cette dernière.
L'article 121-2 du nouveau Code pénal dispose que :

> *« Les personnes morales, à l'exclusion de l'Etat, sont responsables pénalement, selon les distinctions des articles 121-4 à 121-7 et dans les cas prévus par la loi ou le règlement, des infractions commises, pour leur compte, par leurs organes ou représentants.*
> *Toutefois, les collectivités territoriales et leurs groupements ne sont responsables pénalement que des infractions commises dans l'exercice d'activités susceptibles de faire l'objet de conventions de délégation de service public.*
> *La responsabilité pénale des personnes morales n'exclut pas celle des personnes physiques auteurs ou complices des mêmes faits, sous réserve des dispositions du quatrième alinéa de l'article 121-3. »*

Il ne parait pas possible qu'un salarié puisse être considéré comme un représentant de la personne morale qu'est l'entreprise, en effet peuvent être considérés comme représentants uniquement les représentants légaux (comme par exemple le gérant d'une SARL ou le président directeur général d'une SA). Le salarié pourrait tout de même engager la responsabilité pénale de l'entreprise en tant que représentant cette dernière si il justifiait d'une délégation valable des pouvoirs de l'employeur[161].

---

[160] Principe d'ailleurs clairement affirmé par la Cour de cassation : *« Mais attendu que l'article 1384 alinéa 5 du Code civil, généralement édicté pour assurer à la victime d'un dommage la réparation qui lui est due, a, dans son alinéa 5*, spécialement pour but de protéger les tiers contre l'insolvabilité de l'auteur du préjudice en leur permettant de recourir contre son employeur.. ». Cass. Ch. Civ. 6 février 1974.
[161] Voir Cour de cassation, ch. crim. 1 décembre 1998.

En raison du principe qui veut que les dispositions pénales soient d'interprétation stricte[162] toute assimilation extensive par la jurisprudence semble devoir être exclue.
Enfin l'admission de la responsabilité pénale des entreprises n'est possible que si elle a été expressément prévue par les textes, elle répond à un principe de spécialité. Cependant les actes pour lesquelles la responsabilité des personnes morales peut être recherchée sont assez nombreux, notamment : crimes contre l'humanité, homicides, violences involontaires, discrimination, proxénétisme, trafic de drogue, actes de terrorisme, usage irrégulier de la qualité,… (il faut dans ce domaine noter que le projet de loi pour la confiance dans l'économie numérique ajoute le cas de faute dans la conservation des données de connexion).

Certains auteurs ont pu considérer que l'entreprise pourrait voir sa responsabilité pénale engagée sur le fondement de la complicité pour fourniture de moyens[163] prévue aux articles 121-6 et 121-7 du nouveau Code de procédure pénale.
Ces articles disposent :

> ***Article 121-6***
> *Sera puni comme auteur le complice de l'infraction, au sens de l'article 121-7.*
>
> ***Article 121-7***
> *Est complice d'un crime ou d'un délit la personne qui sciemment, par aide ou assistance, en a facilité la préparation ou la consommation.*
> *Est également complice la personne qui par don, promesse, menace, ordre, abus d'autorité ou de pouvoir aura provoqué à une infraction ou donné des instructions pour la commettre.*

L'employeur serait complice de l'infraction commise par son employé du simple fait qu'il ait mis à disposition de ce dernier les moyens matériels d'accomplir ses actes malveillants.
Cependant si cette position peut paraître admissible au premier abord, elle ne résiste pas à une analyse de la mise en cause au titre de la complicité. En effet, en dehors du fait que l'acte principal soit punissable, l'admission de la complicité par fourniture de moyens nécessite une démarche intentionnelle. Il faut donc que les moyens aient été fournis en connaissance de cause (en sachant qu'ils allaient participer à la commission d'une infraction), même s'ils n'étaient pas indispensables à la commission de l'infraction[164].
Ainsi le responsable d'un centre serveur hébergeant des services télématiques, bien que mettant un *« outil entre les mains du fournisseur de services »* n'a pas été déclaré complice de l'outrage aux bonnes mœurs reproché au fournisseur[165].
Dans ces conditions, il ne semble pas que l'employeur puisse être inquiété sur le plan pénal en raison des actes commis par ses salariés grâce à la connexion à l'internet fournie par lui. Il convient de noter que si les dispositions de l'article 32-3-3 lui étaient applicables, il verrait affirmer clairement son irresponsabilité pénale, mais, comme nous avons pu le voir,

---

[162] Prévu par l'article 111-4 du nouveau Code pénal, le principe *poenalia sunt restringenda* est le corollaire du principe de la légalité des peines.
[163] M. Richeveaux, l'introduction de l'internet dans les entreprises, 8 mars 2001. P.5. Disponible sur le site www.droit-technologies.org.
[164] Dans ce sens Cour de cassation, ch. Crim, 22 janvier 1991.
[165] Cour de cassation, ch. Crim., 15 novembre 1990.

l'application de ce régime supposerait que l'entreprise ait conservé les données de connexion de ses employés.

En l'état de notre droit on ne peut que constater le risque civil qui pèse sur les entreprises en raison de la fourniture aux salariés d'un accès à l'internet. Ce risque peut inciter l'employeur à vouloir conserver les données de connexion de ses employés pour tenter de limiter, autant que faire se peut, l'engagement de sa responsabilité. Dans le cas de la jurisprudence Escota l'employeur avait été en mesure de déterminer l'auteur du site litigieux (probablement grâce à la conservation des logs des connexions émises depuis le réseau intranet), on ne peut que s'interroger sur la solution qui aurait été retenue si l'entreprise avait été dans l'impossibilité de le faire. L'état actuel de la jurisprudence montre surtout l'opposition existant entre les régimes de responsabilité des prestataires de l'internet et celui du commettant. Ainsi l'entreprise, si elle peut, en pratique, techniquement être assimilée à un FAI, à raison de la fourniture d'accès à l'internet, répond à des impératifs différents et contradictoires en matière de responsabilité.
On peut alors comprendre que les sociétés, pour éliminer tout risque d'une plus importante mise en cause de leur responsabilité, désirent conserver les logs de leurs salariés. Cependant la législation sociale pourrait être un obstacle à leur désire de conservation.

B. La conservation des traces de connexion à la lumière du droit social

Si l'entreprise se voit contrainte de conserver les logs de ses employés, comme cela est possible, il pourrait en résulter quelques difficultés de mise en œuvre, sur le plan pratique (importance des volumes de données devant être stockées) mais principalement au niveau juridique (compatibilité avec le droit social notamment). En attendant un éclaircissement des textes le doute prédomine, l'employeur se trouve plongé au cœur d'un dilemme : d'un coté il peut être tenté de conserver les données de connexion pour satisfaire à une potentielle obligation légale (il risque de voir engager sa responsabilité envers l'Etat[166]), de l'autre coté, en absence de prescription légale explicite, l'entreprise se doit de respecter les dispositions protectrices des salariés.
En effet si les libertés de citoyens sur l'internet voient leur champ se réduire inextricablement, il n'en est pas de même en ce qui concerne le salarié.
Paradoxalement la vie privée lorsque l'on « surfe » sur la toile depuis son domicile semble moins protégée que celle du salarié qui s'adonnerait à la même activité et à des fins personnelles depuis son poste de travail. Il est devenu constant que la liberté des salariés dans l'entreprise doit être assurée face à l'emprise que pourrait avoir l'employeur : l'employé s'est vu reconnaître le droit à une vie privée au travail sans que l'entreprise ne soit en mesure de s'immiscer ou de contrôler les activités de ses salariés relevant de leur sphère privée.

En raison de l'émergence des nouvelles technologies, le risque d'atteinte à leur vie privée s'est développé considérablement : *« L'évolution aura été constante. D'abord, le contremaître, personne repérable, chargé de contrôler la présence physique du salarié sur son lieu de travail et en activité. Puis, les "contremaîtres électroniques" chargés du contrôle de la présence physique : les badges d'accès. S'ouvre désormais l'ère du "contremaître virtuel" pouvant tout exploiter sans que le salarié en ait toujours parfaitement conscience et*

[166] Pour reprendre les termes de Me Sédallian. La responsabilité de l'employeur en tant que fournisseur internet, Légicom n° 27 2002-2.p. 47.

permettant, le cas échéant, au-delà des légitimes contrôles de sécurité et de productivité des salariés, d'établir le profil professionnel, intellectuel ou psychologique du salarié "virtuel". »[167]

Dès lors, les craintes inspirées par les possibilités de traçabilité, offertes par l'utilisation des systèmes d'information au sein des sociétés, ont conduit les organismes de défense des libertés à adopter une position très protectrice pour les salariés.
La jurisprudence française a suivi le même mouvement, au point que l'on peut être amené à s'interroger sur la compatibilité entre l'obligation de conservation des logs des salariés par l'entreprise et cette protection accrue reconnue aux employés.
Il semble que l'existence d'un lien de subordination, caractérisant le contrat de travail, ait favorisé une stricte application du droit à la vie privée au profit des salariés.

1. Dispositions législatives visant à la protection du salarié face aux nouvelles technologies

Le droit social s'est grandement adapté aux risques que pouvaient représenter les technologies de l'information et de la communication pour les collaborateurs de l'entreprise. Le législateur a donc instauré des mesures ayant pour vocation de limiter les prérogatives de l'employeur devant l'équilibre inégal qui régit les relations salariales. Ces mesures pourraient constituer une entrave à la conservation des traces de connexion.
Certaines dispositions protégeant le salarié, devant le danger que représente l'immixtion des nouvelles technologies dans l'entreprise, ont été prises au niveau Européen.
La recommandation n° R (89) du Comité des Ministres du Conseil de l'Europe[168] aux Etats Membres sur la protection des données à caractère personnel utilisées à des fins d'emploi prévoit en son article 3 que :

> *« 3.1 Conformément aux législations et pratiques nationales et, le cas échéant, aux conventions collectives, les employeurs devraient informer ou consulter leurs employés ou les représentants de ceux-ci préalablement à l'introduction ou à la modification de systèmes automatisés pour la collecte et l'utilisation de données à caractère personnel concernant les employés.*
> *Ce principe s'applique également à l'introduction ou à la modification de procédés techniques destinés à contrôler les mouvements ou la productivité des employés.*
> *3.2 L'accord des employés ou de leurs représentants devrait être recherché avant l'introduction ou la modification de tels systèmes ou procédés, lorsque la procédure de consultation mentionnée au paragraphe 3.1 révèle une possibilité d'atteinte au droit au respect de la vie privée et de la dignité humaine des employés, à moins que d'autres garanties appropriées ne soient prévues par la législation ou la pratique nationale. »*

[167] CNIL, rapport d'étude et de consultation publique, La cybersurveillance des salariés dans l'entreprise, mars 2001.p. 4.
[168] Adoptée par le Comité des Ministres le 18 janvier 1989.

Mais déjà dans l'ordre interne une première limitation législative aux pouvoirs de l'employeur est intervenue le 4 août 1982. Ce fut le règlement intérieur qui subit la première attaque au travers de la modification de l'article 122-35 du Code du travail. La loi 82-689, comme le remarquait alors le professeur Lyon-Caen, *« s'est attaquée à la plus vieille institution du droit du travail : le règlement intérieur, acte dans lequel s'exprime le pouvoir réglementaire privé du chef d'entreprise »*. L'ajout fait à l'article 122-35 dispose que :

> *Article 122-35 : […] Il [le règlement intérieur] ne peut apporter aux droits des personnes et aux libertés individuelles et collectives des restrictions qui ne seraient pas justifiées par la nature de la tâche à accomplir ni proportionnées au but recherché.*
> *[…]*

Cette modification n'avait pas alors pour but d'empêcher l'intrusion que pouvait permettre le recours aux nouvelles technologies dans le monde du travail. Cependant cette première limitation aux pouvoirs de l'employeur permit à la jurisprudence de se développer et a ouvert la voie aux décisions et législations relatives plus particulièrement aux TIC. En imposant le principe de proportionnalité comme contrepoids à l'omnipotence du chef d'entreprise, la loi de 1982 posait une première pierre qui allait ensuite permettre de construire une barrière à l'ingérence de l'employeur dans la vie privée du salarié.

Un second pas fut opéré par loi du 31 décembre 1992 qui généralisa le principe de proportionnalité. Ainsi le nouvel article 120-2 inséré dans le Code du travail prévoit que :

> *« Nul ne peut apporter aux droits des personnes et aux libertés individuelles et collectives de restrictions qui ne seraient pas justifiées par la nature de la tâche à accomplir ni proportionnées au but recherché. »*

Dans le même temps, l'article 122-39 a soumis au même régime juridique que le règlement intérieur lui-même toutes les notes de service ou tout autre document qui portent prescriptions générales et permanentes dans les matières qui relèvent du règlement intérieur, c'est-à-dire notamment les conditions d'utilisation des équipements de travail et les règles générales et permanentes relatives à la discipline.

Parallèlement la même loi a imposé l'obligation pour l'employeur d'informer et de consulter le comité d'entreprise, avant toute mise en œuvre de moyens techniques permettant un contrôle de l'activité des salariés. C'est ce qu'il ressort de l'article 432-2-1 qui dispose que :

> *« Le comité d'entreprise est informé, préalablement à leur utilisation, sur les méthodes ou techniques d'aide au recrutement des candidats à un emploi ainsi que sur toute modification de celles-ci.*
> *Il est aussi informé, préalablement à leur introduction dans l'entreprise, sur les traitements automatisés de gestion du personnel et sur tut e modification de ceux-ci.*

Le comité d'entreprise est informé et consulté, préalablement à la décision de mise en œuvre dans l'entreprise, sur les moyens ou les techniques permettant un contrôle de l'activité des salariés. »

Dans le même ordre d'idée l'article 432-2 imposait quant à lui :

« Le comité d'entreprise est informé et consulté, préalablement à tout projet important d'introduction de nouvelles technologies, lorsque celles-ci sont susceptibles d'avoir des conséquences sur l'emploi, la qualification, la rémunération, la formation ou les conditions de travail du personnel. Les membres du comité reçoivent, un mois avant la réunion, des éléments d'information sur ces projets et leurs conséquences quant aux points mentionnés ci-dessus.
Lorsque l'employeur envisage de mettre en œuvre des mutations technologiques importantes et rapides, il doit établir un plan d'adaptation. Ce plan est transmis, pour information et consultation, au comité d'entreprise en même temps que les autres éléments d'information relatifs à l'introduction de nouvelles technologies. En outre, le comité d'entreprise est régulièrement informé et périodiquement consulté sur la mise en œuvre de ce plan. »

Il ressort de toutes ces dispositions, directement ou indirectement relatives à la place des technologies de l'information et de la communication, que l'employeur ne peut agir unilatéralement, son pouvoir est limité par les textes.

On considère généralement que la mise en place de nouveaux moyens technologiques dans l'entreprise doit répondre à trois types d'exigences.

- La première est la proportionnalité induite par l'article 120-2 du Code du travail. Il vise d'une manière générale le respect de droits des personnes et forme le prolongement des principes de la loi informatique et libertés[169].

- La seconde est la transparence, également issu de la loi informatique et libertés qui impose qu'aucune donnée ne peut être collectée par un moyen frauduleux ou illicite. Cela se traduit par une obligation d'information des personnes à l'endroit desquelles s'effectuent la collecte et le traitement, sur les destinataires des traitements et sur le lieu où s'exercent les droits d'accès et de rectification. Le même principe a été transposé au monde l'entreprise au travers de l'article 121-8 qui dispose qu' *« aucune information concernant personnellement un salarié ou un candidat à un emploi ne peut être collectée par un dispositif qui n'a pas été porté préalablement à la connaissance du salarié ou du candidat à un emploi. »*

- Enfin la dernière est la discussion collective, *« organisée par le Code du travail lors de l'introduction dans l'entreprise de traitements automatisés de gestion du personnel ou de moyens et techniques permettant un contrôle d'activité du salarié (article L 432-2-1 du Code du travail), la discussion collective donne sa substance au principe de*

[169] Loi du 6 janvier 1978, n° 78-17 relative à l'informatique, aux fichiers et aux libertés.

proportionnalité. Le rapport inégal entre l'employeur et ses salariés, consubstantiel à la nature même du contrat de travail et au lien de subordination qui le caractérise, ne garantit pas naturellement la proportionnalité. Trop souvent, sous l'influence sans doute des entreprises américaines, les employeurs soumettent individuellement aux salariés, des chartes, des engagements écrits équivalant à une abdication complète par les salariés de leurs droits. »[170]

Ces trois grands principes ont été interprétés de manière extensive par la jurisprudence et ont permis de créer un véritable espace de liberté au profit des salariés.
Tel a été notamment l'apport, concernant l'usage de l'internet[171], du célèbre arrêt Nikon[172]qui énonce que la salarié dispose du droit, *« même temps et au lieu de travail, au respect de l'intimité de sa vie privée*[173] *»* et que donc *« l'employeur ne peut (...) prendre connaissance des messages personnels émis par le salarié et reçus par lui grâce à un outil informatique mis à sa disposition pour son travail et ceci, même au cas où l'employeur aurait interdit une utilisation non professionnelle de l'ordinateur ».*

Les décisions de justice sanctionnant le non respect, par l'employeur, de ces trois limites à son pouvoir sont légion. Elles se caractérisent par une invalidation de la preuve obtenue de façon déloyale à l'encontre des salariés comme l'illustre l'arrêt Néocel[174] de la Cour de cassation qui, tout en affirmant le droit de l'employeur de contrôler et surveiller l'activité de ses salariés pendant le temps de travail, pose le principe que tout enregistrement d'images ou de paroles à l'insu des salariés constitue un mode de preuve illicite.

Sans s'appesantir plus avant sur les droits reconnus aux collaborateurs pendant leur temps de travail (ce qui sortirait du cadre de cette étude), on peut aisément s'apercevoir que la protection des salariés dans leur vie personnelle[175] constitue un sérieuse entrave à l' « omnipotence » du chef d'entreprise.

Il convient aussi de ne pas négliger les limitations, qui ne sont pas propres au domaine de l'entreprise, comme celles relatives au traitement automatisé des données à caractère personnel. La loi de 1978[176] instaure des procédures de déclaration des traitements et impose

---

[170] CNIL, rapport d'étude et de consultation publique, La cybersurveillance des salariés dans l'entreprise, mars 2001. p. 18.
[171] Dans un contexte plus général d'autres décisions antérieures avaient déjà affirmé l'existence d'une vie privée au travail. Notamment CEDH, N c. Allemagne, 23 novembre 1992.
[172] Cour de cassation, ch. Soc. 2 octobre 2001.
[173] L'arrêt vise la vie privée alors que l'on parle déjà d'une vie personnelle au travail. *« Si l'expression vie personnelle du salarié a été substituée à celle de vie privée, ce n'est aucunement pour éliminer cette dernière, mais pour aller au-delà. La vie privée telle qu'elle est protégée par l'article 9 du Code civil et par l'article 8 de la CEDH, concerne essentiellement l'intimité de la vie humaine : la liberté du domicile, le droit au respect et à l'inviolabilité des correspondances, le droit à la vie sexuelle et à une vie familiale normale. La vie personnelle, qui inclut l'intimité de la vie privée, englobe aussi d'autres aspects de la vie du salarié et notamment ses démarches publiques : les lieux publics qu'il fréquente, les associations ou partis politiques auxquels il adhère, ses activités culturelles ou sportives, ses lectures ou les opinions qu'il exprime. »* Ph. Waquet, les libertés dans l'entreprise, RJS 2000. p. 335.
[174] Cour de cassation, chambre sociale, 20 novembre 1991.
[175] Pour reprendre les termes utilisés par la Cour de cassation.
[176] Loi du 6 janvier 1978 n° 78-17 relative à l'informatique, aux fichiers et aux libertés. Cette loi a d'ailleurs créé une autorité administrative indépendante chargée de veiller au respect des libertés des individus : la CNIL.

des conditions de licéité (droit d'accès, de rectification, sécurité des traitements,…). Ces dispositions sont d'ailleurs pénalement sanctionnées[177] et prévoient la possibilité de la mise en cause de la responsabilité pénale des personnes morales.

Il est clair que la conservation des données de connexion des salariés doit faire l'objet d'une déclaration à la CNIL, mais celle-ci prône également un contrôle aussi limité que possible de l'activité des salariés sur l'internet. Elle considère ainsi qu' *« un contrôle a posteriori des données de connexion à internet, de façon globale, par service ou par utilisateur ou un contrôle statistique des sites les plus visités devrait dans la plupart des cas être suffisant sans qu'il soit nécessaire de procéder à un contrôle nominatif individualisé des sites accédés »*[178]. De plus la CNIL s'est montrée réticente à une conservation, pour une durée trop importante, des traces de connexion ; elle estime ainsi : « *Un souci d'équilibre et de proportionnalité a convaincu la CNIL qu'une durée de conservation limitée à trois mois pour les données de connexion à Internet serait adaptée à l'ensemble des intérêts en cause »*[179]. L'employeur dans le doute pourrait désirer conserver les logs pour la durée maximale prévue par les dispositions législatives (un an, à moins que les décrets à paraître ne conviennent autrement), ici encore sa démarche serait en désaccord avec les principes affirmés par l'autorité en charge de la protection des données personnelles.

Face à l'ensemble de ces dispositions et en l'absence d'obligation légale claire l'employeur se voit mis dans une situation ambiguë et contradictoire, entre besoin de conservation des traces de connexion et obligations légales encadrant strictement les conditions de ce contrôle.

2. La position inconfortable du chef d'entreprise

L'employeur se retrouve dans une situation pour le moins délicate, car comme nous l'avons vu[180], il n'existe pas d'obligation légale précise lui imposant de conserver les données de connexion de ses employés. En l'absence de décret fixant les modalités d'application des articles 43-9 et 32-3-1[181], il ne peut savoir s'il lui appartient ou non de prendre des mesures dans ce sens. Même s'il voulait adopter une position prudente, en décidant de détenir les traces de ses employés, il pourrait éprouver de grandes difficultés, voire se trouver dans l'impossibilité de le faire.

Il est en effet difficile de considérer que, sans texte le prévoyant, l'employeur puisse raisonnablement répondre au principe de proportionnalité.
Qui plus est, sa démarche serait en opposition avec les principales recommandations adoptées par les organismes faisant autorité dans le domaine de l'internet et de la protection des données personnelles[182]. Les différents rapports relatifs à la cybersurveillance des salariés plaident en effet pour un contrôle limité de l'utilisation faite par les salariés de la connexion à l'internet fournie par l'employeur.

---

[177] Les sanctions sont celles figurant aux articles 226-16 à 226-24 du Code pénal.
[178] CNIL, la cybersurveillance sur les lieux de travail, 5 février 2002. p. 10.
[179] CNIL, rapport d'activité pour l'année 2001, éditions la Documentation Française, p.22.
[180] Voir chapitre I, B p. 33.
[181] Respectivement de la loi 2000-719 et de la LSQ (voir supra chapitre 1 A). p.23
[182] A savoir la CNIL et le Forum des Droits sur l'internet (voir leurs rapports sur la cybersurveillance des salariés respectifs).

La CNIL en pratique s'autorise à refuser la délivrance des récépissés lors d'un dépôt de déclaration du traitement automatisé de données à caractère personnel, elle pourrait donc s'opposer à la conservation des logs par l'employeur lors de l'accomplissement de cette démarche obligatoire. Il faut d'ailleurs noter que l'Autorité a déjà usé de son influence dans un domaine connexe, celui des autocommutateurs téléphoniques, en élaborant le 20 décembre 1994 une norme simplifiée constituant l'encadrement juridique et précisant les règles minimales applicables à leur usage.

La conservation des traces de connexion dans l'entreprise se heurte donc aux grands principes instaurés à l'initiative du législateur et relayés par certaines autorités.

L'utilisation de l'internet dans les entreprises a été régulée au travers de l'adoption de chartes. Celles-ci n'ont normalement pas de valeur contraignante mais elle en acquiert une par leur adjonction au règlement intérieur de l'entreprise[183]. Ces chartes prévoient les modalités de l'usage de la connexion (à des fins privées ou non), elles organisent l'information des salariés sur les contrôles existants. L'adoption de ces chartes est souvent l'occasion d'âpres discussions entre les représentants des salariés et l'employeur pour trouver une solution qui puisse être susceptible de satisfaire les deux parties en présence.
La décision prudente de l'employeur qui désirerait conserver les traces de connexion de ses employés (dans la crainte que dans l'impossibilité de déterminer le coupable il voit sa responsabilité encore plus fortement engagée), serait l'occasion d'un nouveau conflit avec les représentants du personnel. Il est évident que les représentants syndicaux verront d'un mauvais œil une conservation des traces de connexion qui permettrait à l'employeur de connaître chaque agissement de ses collaborateurs sur l'internet de façon précise et nominative.
Même si une obligation légale venait à être affirmée il est hautement probable que la société verrait quelques difficultés à instaurer, dans un climat social serein, les mesures de rétention des données de connexion pour la durée maximale voulue par le législateur.

Enfin un dernier obstacle pourrait être constitué par le contrôle que doit exercer l'inspecteur du travail sur le règlement intérieur (et donc sur la charte internet qui y est annexée). En effet l'employeur doit lui transmettre le projet de règlement ainsi que l'avis du Comité d'Entreprise[184]. « *L'inspecteur peut exiger le retrait ou la modification des dispositions contraires aux articles L 122-34, L 122-35 et L122-39-1, c'est à dire les clauses :*

- *visant des matières non prévues par la loi ;*
- *ne respectant pas les règles linguistiques ;*
- *non conformes aux lois, règlements, conventions et accords collectifs ;*
- *contraires aux droits des personnes et aux libertés ou discriminatoires »*[185].

Ce contrôle peut être exercé au moment de l'adoption du règlement mais aussi de manière permanente, à n'importe quel instant.

---

[183] L'article 122-39 du Code du travail qui dispose que *« les notes de service ou tout autre document qui portent prescriptions générales et permanentes dans les matières mentionnées à l'article 122-34 sont, lorsqu'il existe un règlement intérieur, considérées comme des adjonctions à ce règlement intérieur »* permet lorsque la charte comporte un volet disciplinaire de l'intégrer au règlement intérieur. Il acquiert ainsi une valeur contraignante.
[184] Article L 122-36 à 38 du Code du travail.
[185] Memento Social 2003, éditions Francis Lefebvre, n° 7536 et S.

Il se pourrait qu'un inspecteur de travail, sensible aux positions adoptées par la CNIL, déclare que la disposition visant à la conservation des logs doit être supprimée au motif qu'elle est « contraire aux droits des personnes ».

En réalité, l'employeur se retrouve dans une position délicate, la conservation des logs nécessite qu'il respecte les dispositions propres au droit social à savoir le principe de proportionnalité[186] (qui pourra difficilement être respecté en absence d'obligation légale précise), le principe de transparence[187] (qui devra sans doute prendre la forme d'une modification de la charte internet de l'entreprise avec les difficultés pratiques que cela ne manquera pas d'entraîner) et enfin le principe de discussion collective[188] qui veut que toute introduction d'un traitement automatisé des données permettant un contrôle de l'activité des salariés dans l'entreprise soit faite après information du Comité d'Entreprise.
En pratique, tant que le législateur n'impose pas de façon claire et non équivoque une obligation de conservation des traces pour l'entreprise, comment cette dernière peut-elle l'opposer à la CNIL, à l'inspection du travail et à ses salariés ? Parallèlement, si elle décide de ne pas détenir les données de connexion, comment pourra-t-elle se justifier devant les forces de l'ordre qui considèrent le principe de conservation comme acquis ?
Il est probable que même si l'employeur se voyait contraint, par une obligation légale, de conserver les données de connexion il resterait soumis à ces dispositions, seul le principe de proportionnalité serait automatiquement rempli (la conservation se trouvant justifiée par une obligation légale).

La mise en place d'un tel traitement nécessiterait enfin une déclaration auprès de la CNIL qui risque de ne pas l'autoriser en l'absence de textes légaux l'imposant clairement, sa position étant de limiter tout contrôle de l'activité des salariés dans l'usage qu'ils peuvent faire de l'internet.
Pourtant il est clair que la reconnaissance d'une sphère de liberté aux collaborateurs aura pour conséquence une volonté de l'employeur de se délester de sa responsabilité en cas d'actes malveillants commis par ses salariés, de la même manière que les prestataires de l'internet en rétablissant la traçabilité ont pu se voir reconnaître irresponsables des actes commis par leur usagers sur le net. Suivant le même cheminement l'employeur *« sera nécessairement conduit à rendre le salarié responsable de l'usage qu'il fait de ce domaine réservé (sa sphère de liberté) »*[189] et donc à conserver les traces de connexion de ses employés.

Il convient, en dernier lieu, de noter que l'application du régime propre aux prestataires de l'internet pourrait poser un problème aux entreprises, si l'on convient que celles-ci doivent détenir les données de connexion de leur employés en vertu de l'article 29 de la LSQ (insérant l'article 32-3-1 dans le Code des postes et télécommunications), cela implique aussi qu'elles ne doivent en aucun cas conserver les contenus des pages visitées ou des correspondances échangées, la contravention à cette disposition étant assortie de sanctions pénales. Or la loi n'a pas prévu le cas particulier des entreprises, en effet celle ci peut voir transiter par son réseau deux types de messages : des messages privés ou professionnels. La

[186] Article 120-2 du Code du travail.
[187] Article 121-8 du Code du travail.
[188] Article 432-2-1 du Code du travail.
[189] A. Supiot, Travail, droit et technique, revue Droit social, numéro spécial, droit du travail et nouvelles technologies de l'information et de la communication. p. 25.

loi ne fait pas la distinction, une application stricte empêcherait dons la société de conserver et d'archiver les messages professionnels (dont la conservation pourrait être requise à titre de preuve d'une transaction). Tel est le cas notamment en matière bancaire en ce qui concerne la preuve des ordres échangés (archivage pendant 5 ans). Plus encore, l'employeur pourrait être amené à garder l'ensemble des e-mails (professionnels et privés) devant le risque qu'un message destiné à l'entreprise n'ait été, par mégarde, désigné comme étant personnel.
L'application du régime des prestataires de l'internet aux sociétés ne va pas sans poser de multiples difficultés.

Conclusion

L'émergence de nouvelles technologies ne va pas sans poser de nouvelles questions pour le juriste qui doit sans cesse tenter de concilier le corpus de règles existantes avec les impératifs induits par les outils technologiques récents. Tel est le cas de l'utilisation de la technologie NAT qui n'autorise pas un contrôle extérieur permettant de retracer l'origine précise des communications émises depuis un réseau d'entreprise, faisant ainsi disparaître des dizaines de milliers d'ordinateurs de toute possibilité de traçage.
Sans aller jusqu'à soutenir que *« le droit, principalement celui des libertés individuelles, n'a pas à s'incliner devant l'état de la technologie ; c'est à la technologie de s'adapter (et elle en est très capable) aux exigences fondamentales du droit »*[190], le juriste ne peut ignorer les enjeux induits par les NTIC, il convient, à notre avis, non pas de limiter la technique en fonction de notre droit, mais plutôt d'adapter notre droit (et nous en sommes capables) aux nouvelles technologies.

Tel est l'enjeu que représente l'introduction de l'internet dans le monde du travail, l'importance des infrastructures mises en place, conduit à s'interroger sur la possibilité de considérer la société comme un prestataire internet comme les autres devant être soumis aux mêmes obligations que ces derniers.

L'entreprise peut elle être ainsi assimilée à un fournisseur d'accès internet ? Dans ce cas est elle soumise à l'obligation de conservation des données de connexion imposée aux FAI ? En l'état actuel de notre droit il est difficile de répondre à ces questions ; mais il demeure que, si l'entreprise devait être considérée comme un fournisseur d'accès, elle ne serait pas un prestataire comme les autres. En effet le monde du travail reste soumis à des dispositions spéciales souvent incompatibles avec les dispositions légales prévoyant la conservation des données de connexion en contrepartie d'une irresponsabilité.
L'existence d'un lien de subordination, qui est l'élément fondamental de la relation employeur/employés, induit la mise en place de mesures spécifiques afin de protéger le salarié placé en état de faiblesse.
Ainsi la détention des traces des collaborateurs se voit limitée par les dispositions légales assurant la protection des salariés dans leurs vies personnelles, qui se trouve étendue à leur cadre de travail.
Parallèlement l'entreprise répond à un régime spécial de responsabilité civile pour autrui (article 1384 alinéa 5) renforcé encore par la jurisprudence, contrairement aux fournisseurs d'accès qui se verront reconnaître une responsabilité très atténuée par la future loi pour la confiance dans l'économie numérique.
Cette situation place les sociétés offrant une connexion à l'internet à leurs employés dans une position inconfortable. Le régime de responsabilité qui leur est propre demeure inadapté aux risques qu'engendre la communication sur un réseau mondial et en totale opposition avec celui applicable aux prestataires de l'internet. En effet, comme nous avons pu le voir au cours de cette étude, en l'état, les deux régimes de responsabilité répondent à des impératifs totalement différents, pour ne pas dire antinomiques (responsabilité étendue pour l'employeur pour protection des victimes/ irresponsabilité pour les prestataires simples intermédiaires).

[190] G. Lyon-Caen, commentaire de l'arrêt Nikon du 2 octobre 2001. J. E. Ray, Adde, Sem. Soc. Lamy, n° 1046, commentaire de G. Lyon-Caen. Précit.

Comment concilier ces deux régimes a priori antagonistes ?

Il est peu probable que les développements jurisprudentiels apportés à l'article 1384 alinéa 5, soient remis en cause en ce qui concerne la fourniture d'accès par l'entreprise. La décision Escota (sous réserve qu'elle soit confirmée) marque bien la tendance adoptée par les tribunaux vers une extension encore accrue du régime de responsabilité des commettants.
On peut penser qu'il ne sera pas possible d'appliquer le principe d'irresponsabilité des FAI (même si le futur texte de l'article 32-3-3 semble assez large pour pouvoir recouvrir les réseaux d'entreprise) en raison du cadre particulier dans lequel l'employeur offre l'accès à l'internet à ses salariés (lien de subordination, protection de la victime).
Il parait cependant souhaitable d'alléger la responsabilité de la société, mais il faudra sans doute que cette atténuation se fasse en accord avec les principes dégagés par la jurisprudence relativement à l'article 1384 alinéa 5.
L'application aux entreprises de l'obligation de conservation de traces pourrait permettre de justifier une mise en cause moindre de leur responsabilité. Cependant, si l'application du régime de responsabilité des prestataires de l'internet se heurte à des antagonismes liés au cadre particulier du monde du travail, il semble que l'obligation de détention des données de connexion des salariés par l'entreprise ne puisse, quant à elle, être écartée.
La traçabilité s'impose désormais comme un principe général qui a vocation à recouvrir l'ensemble des communications effectuées au travers de l'internet. Est-il possible d'envisager que l'on laisse subsister des zones non régulées où l'anonymat serait assuré ? Ce serait admettre qu'il existe des cas dans lesquels l'auteur d'une infraction ne peut être recherché et qu'il peut agir en toute impunité sous couvert de l'anonymat offert par le réseau NAT. Les évolutions législatives ne militent pas pour cette thèse, au contraire la détermination de l'auteur de tout comportement fautif sur le net est devenue une priorité.
Cependant la conservation des données de connexions au sein de l'entreprise impose aussi quelques ajustements. Ainsi l'employeur doit être en mesure de contrôler l'activité de ses salariés. Il est difficilement envisageable de considérer que l'entreprise ne puisse vérifier les conditions dans lesquelles ses employés utilisent la connexion à l'internet, principalement l'usage fait à titre privé de celle-ci.
Les chartes adoptées dans les sociétés soumettent généralement le droit à une utilisation personnelle à un usage raisonnable. Il convient donc de reconnaître à l'entreprise le droit d'exercer un contrôle sur l'application pratique de cette limitation. La Cour de cassation a d'ailleurs affirmé clairement ce principe en énonçant que : *« l'employeur a le droit de contrôler et de surveiller l'activité de ses salariés pendant le temps de travail (...) seul l'emploi de procédé clandestin est illicite »*[191]. Or l'article 29 de la LSQ ne prévoit la détention de ces données que *« pour mise à disposition de l'autorité judiciaire »* et non du chef d'entreprise. Ce dernier se verrait il alors interdit d'accéder aux logs dans le cadre du contrôle, pourtant légitime, de l'usage fait de l'internet par ses subordonnés ?
Plus encore la même disposition (article 29 de la LSQ) prévoit l'effacement (ou l'anonymisation) des contenus des communications échangées au travers de l'internet. Il en résulte une grande difficulté pour l'employeur qui sera alors dans l'impossibilité d'archiver les messages échangés et, la loi ne faisant pas la distinction, cette interdiction pourrait être étendue à ceux reçus ou émis à titre professionnel. Cela pourrait avoir pour conséquence un

[191] Cour de cassation, ch. soc. 14 mars 2000.

profond handicap en terme de productivité des entreprises, les correspondances électroniques ne pouvant alors être conservées notamment à titre de preuve.
Il faut enfin noter qu'il est évident que la conservation des traces aura un coût non négligeable pour les sociétés, il est peu probable que l'Etat aille jusqu'à indemniser les grandes entreprises en contrepartie de l'obligation de conservation des logs.

Quelles pourraient être les solutions apportées à ces points de friction ?

La LSQ limite l'accès aux données de connexion recueillies par les prestataires afin que ces derniers ne puissent utiliser ces informations à des fins commerciales (vente de fichiers client) ou ne portent atteinte à la vie privée de leur utilisateurs. Or cette protection, dans le cas des salariés, est déjà assurée par le droit social et les diverses positions de la CNIL (dans le cadre de la déclaration des traitements automatisés de données notamment). La protection des salariés étant déjà assurée il semble superflu d'imposer à l'employeur de respecter celle prévue par la LSQ.

Concernant la charge financière que représente l'indemnisation des entreprises qui seraient conduites à conserver les logs, on peut imaginer que celle-ci se fasse au prorata de la durée de conservation prévue par la charte internet.
Si l'Etat venait à imposer la durée maximale de rétention de douze mois, alors que la politique de l'entreprise la fixe à trois mois en vertu de la charte, la compensation ne pourrait viser que l'écart entre les deux (en l'occurrence neuf mois) ce qui réduirait d'autant la charge financière assumée par l'Etat. Il faudrait prévoir que, durant cette période, l'employeur ne pourra disposer des données de connexion dans le but de contrôler l'activité de ses salariés (le contrôle devant se dérouler uniquement dans le délai de trois mois, dans notre exemple, prévu par la charte).

Annexes

Glossaire des termes techniques

- ***Backbone :*** d'après le Vocabulaire de l'informatique et de l'internet paru au Journal officiel du 16 mars 1999: Partie principale d'un réseau de télécommunication ou de téléinformatique, caractérisée par un débit élevé, qui concentre et transporte les flux de données entre des réseaux affluents.

- ***Déni de service :*** denial of service en anglais. Attaque pratiquée par des pirates informatique visant à submerger un serveur de requêtes dans le but d'entraver son fonctionnement et de le rendre inactif. Ce type d'attaque utilise souvent plusieurs machines afin de littéralement inonder le serveur victime. On parlera alors d'attaque distribuée.

- ***Email :*** mèl ou courriel sont les termes français consacrés. Service fournit par l'internet permettant de faire transiter des messages, sous forme de texte le plus souvent (bien que l'on puisse aussi ajouter des images, sons,…). Il existe différents services permettant l'acheminement des « mails » comme POP, SMPT, IMAP.

- ***Hacking :*** le hacking est le terme anglais consacré pour ce que l'on dénomme piratage. Cependant il existe une distinction en anglais que l'on ne retrouve pas en français sous le terme générique de piratage. On distingue donc le hacking qui consiste en la prise de contrôle ou l'intrusion dans un système d'information, du cracking qui consiste à supprimer des protections anti-copie sur des œuvres protégées.

- ***Intranet :*** d'après le Vocabulaire de l'informatique et de l'internet paru au Journal officiel du 16 mars 1999: Réseau de télécommunication et de téléinformatique destiné à l'usage exclusif d'un organisme et utilisant les mêmes protocoles et techniques que l'internet.

- ***Log :*** les logs sont des fichiers, souvent au format texte, retraçant les activités ou autres informations qui ont été effectué sur un système d'information. Ces logs pourront contenir des informations sur les changements intervenus sur le système (log système) ou sur les connexions faites par les utilisateurs du réseau (log des connexions). Ces fichiers sont plus ou moins détaillés, mais ils retracent en général : le type d'information demandée ou reçue, l'auteur, la date et l'heure.

- ***Passerelle :*** point du réseau (nœud) servant de lien avec l'extérieur. la passerelle sert à connecter un réseau avec un autre (l'internet), elle permet de relier plusieurs types de réseaux (réseau hétérogènes) par exemple la passerelle permettra de relier un réseau d'entreprise de type ethernet avec un réseau de type différent comme l'internet (TCP/IP). Souvent cette passerelle sera constituée d'un routeur.

- ***Peer to peer :*** (ou point à point, pair à pair, P2P) mode de connexion permettant notamment l'échange de fichiers (musique, film, progiciels) en mettant en relation directe deux ordinateurs distants. Le P2P est très en vogue depuis quelques années grâce au développement des formats MP3 et Div-x. L'utilisation de ce service requiert généralement un petit programme pour l'échange de fichiers, les sites comme le défunt Napster, ou encore Kazaa ou Edonkey établissent un annuaire recensant les fichiers disponibles au téléchargement et leur emplacement.

- ***Protocole :*** ensemble de règles fixant les modalités d'un échange (entre deux ordinateurs). On pourrait comparer le protocole informatique à celui que nous utilisons, de manière innée, pour la communication entre êtres humains (ne pas parler en même temps que son interlocuteur, céder la parole,…)

- ***Proxy :*** serveurs, souvent hébergés par les fournisseurs d'accès à l'internet (mais pas exclusivement), stockant les pages les plus souvent demandées par les utilisateurs. Ce stockage a une double fonction, premièrement d'accélérer les consultations de pages (conservées localement elle seront plus rapidement accessibles), deuxièmement, de faire des économies de bade passante pour les fournisseurs d'accès (souvent facturée au volume des informations échangées).

- ***Routeur :*** élément matériel (hardware) ou implanté sur une machine (software) permettant l'acheminement des données sur l'internet notamment. Le routeur permet de faire transiter les paquets (c'est à dire les données) en choisissant la meilleure "route" possible. Pour cela le routeur dispose d'une table de routage recensant les chemins possibles (les nœuds réseau qui lui sont voisin), en cas d'encombrement il pourra choisir de faire transiter les paquets par un autre chemin.

- ***Virus :*** c'est un petit programme en général le plus léger possible (quelques kilo-octets) dont le but est de se reproduire à l'infini. Il peut occasionner des dégâts si il a été programmé dans ce sens (time bomb par exemple). Il pollue la machine hôte

en se reproduisant dans tous les fichiers. Il est remarqué, quand il n'a pas de vocation plus destructrice, par une activité CPU et/ou mémoire injustifiée.

- ***Vers :*** souvent assimilés aux virus ils s'en distinguent par leur mode de propagation. Les vers se propagent d'un ordinateur à l'autre en utilisant le réseau (l'internet), ils recherchent par exemple les adresses e-mails contenues dans le carnet d'adresse pour se répandre par la messagerie électronique et ce de manière automatique. Le vers peut disposer de mécanismes malveillants qui auront pour but de détruire des données ou de paralyser la machine hôte. Ce qui caractérise le vers par rapport au virus est son mode de propagation (automatique pour le vers/insérée en pièce jointe à un message pour le virus)

- ***Troyen :*** ou cheval de Troie. Programme qui une fois installé sur un ordinateur (souvent en raison de la négligence de l'utilisateur) va avoir pour effet de créer une possibilité pour l'émetteur de prendre le contrôle de la machine du destinataire (on dit qu'il ouvre une *backdoor*). Ce type d'attaque peut ensuite permettre en prenant le contrôle de la machine distante (ouvre un *shell*) de lancer par la suite des attaques distribuées.

Bibliographie

Documents techniques

PUJOLLE Guy, *Initiation aux réseaux*, Edtions Eyrolles, Paris Décembre 2001

GOUPILLE Pierre Alain, *Technologie des ordinateurs et des réseaux* 6ème édition, Editions Dunod, Paris Décembre 2001

CERF Vinton G., *Technical writings*.. Disponible sur le site de Worldcom (www.worldcom.com/fr/ressources/cerf_up/technical_writings).

Autorité de réglementation des télécommunication (ART), *Rapport sur le marché des infrastructures de desserte en fibres optiques haut débit / février 2002,* publication octobre 2002

Rése@ux.74, *network address translation, LE NAT !,* numéro 4 mars 2000

Maged Giurgius, *An Investigation on: NETWORK ADRESS TRANSLATOR (NAT)*, March 25, 2002

Srisuresh P., Holdrege M. *IP Network Address Translator (NAT) Terminology and Considerations,* Lucent Technologies, Internet RFC/STD/FYI/BCP Archives

Documents juridiques

Ouvrages

SEDAILLAN Valérie, *Droit de l'internet,* collection AUI, Editions Net Press, Paris janvier 1997

FERAL-SCHUHL C., *Cyber Droit. Le droit à l'épreuve de l'internet*, Editions Dalloz – Dunod, 1999

Memento social, Editions Francis Lefebvre, 2003

Lamy Droit social, Editions Lamy, mars 2003

Rapports

Conseil d'Etat, *internet et les réseaux numériques,* Les études du Conseil d'Etat, La Documentation Française, 2 juillet 1998

Forum des droits sur l'internet, *Rapport final relations de travail et Internet,* 17 septembre 2002 disponible sur www.foruminternet.org

Forum des droits sur l'internet, *Recommandation aux pouvoirs publics, conservation des données relatives à une communication,* 18 septembre 2001
Forum de droits sur l'internet, *rapport d'activité,* la documentation française 2003

Forum des droits sur l'internet, Synthèse du forum de discussion, *peer to peer : quelle utilisation pour quels usages,* 20 mars 2003

CNIL, *Rapport d'étude et de consultation publique, la cybersurveillance des salariés dans l'entreprise,* Mars 2001 disponible sur www.cnil.fr

CNIL, *Rapport la cybersurveillance sur les lieux de travail,* 5 février 2002 disponible sur www.cnil.fr.

CNIL, *21ème rapport d'activité*, la documentation Française, Paris 2001.

CNIL, *22ème rapport d'activité*, la documentation Française, Paris 2002.

CNIL, *23ème rapport d'activité*, la documentation Française, Paris 2003.

Périodiques

Guide permanent droit et internet, éditions F Lefebvre, mis à jour de manière continue.

Droit social, *Droit du travail et nouvelles technologies de l'information et de la communication,* Numéro spécial sous la direction de J-E Ray, N° 1 janvier 2002

Légicom, N° 27, 2002/2
N° 21/22, 2000/1 et 2

Légalis.net, *e-démocratie, internet et la vie privée au bureau,* N°1 2002, trimestriel, édition des Parques

Expertise des systèmes d'information, N° 257, mars 2002

Textes législatifs

Loi relative à la liberté de communication n° 86-1067 du 30 septembre 1986

Loi relative à la communication audiovisuelle n° 2000-719 du 1er août 2000 modifiant la loi relative à la liberté de communication

Loi sur la sécurité quotidienne n° 2001-1062 du 15 novembre 2001

Loi de Finance Rectificative pour 2001 n° 2001-1276 du 28 décembre 2001

Loi sur la Sécurité Intérieure n° 2003-239 du 18 mars 2003

Projet de loi pour la Confiance dans l'Economie Numérique

Projet de loi portant adaptation de la justice aux évolutions de la criminalité

Sites internet

www.juriscom.net

www.droit-ntic.org

www.droit-technologie.org

www.foruminternet.org

www.telecom.gouv.fr

www.internet.gouv.fr

www.legifrance.fr