http : // www.droit-technologie.org

Présente :

LA CYBERSURVEILLANCE ET LE SECRET PROFESSIONNEL : PARADOXES OU CONTRADICTIONS ?

Maximilien AMEGEE

Juriste

maxamegee@hotmail.com

Date de mise en ligne :15 novembre 2002

Mémoire de Maximilien Dotsé AMEGEE, sous la direction de Monsieur le Professeur De La PRADELLE - Année universitaire 2001-2002

Université Paris X, Nanterre - UFR de Sciences juridiques
DEA de Théorie générale et philosophie du Droit

Je voudrais, si c'est encore permis à l'ère des Nouvelles technologies, remercier Dieu de m'avoir donné la force et le courage d'accomplir ce travail pendant lequel, d'ailleurs, je perdais mon père.

Mes remerciements vont également à Madame, Messieurs, les Professeurs Sylvia LAUSSINOTTE Géraud DE LA PRADELLE, Gilles DARCY et Michel TROPER ; à M. J. FERRI, officier de gendarmerie ; à toute l'équipe de la CNIL et en particulier à Madame de SORBIER et Monsieur LYM ; à toute l'équipe de ENLIVE.FR NET SOLUTION, société d'informatique et de commerce électronique où j'ai véritablement fait mes premiers pas de juriste des NTIC ; à MM. Demba DIALLO, consultant en télécom et chercheur en e-business, Safiou RADJI, expert-comptable ; à Me J. MISSINHOUN, avocat E&Y…

Ceci n'aurait pas été possible sans votre bonne volonté et votre disponibilité à mon égard.

Je n'oublie pas toute l'équipe enseignante du DEA de Théorie générale et philosophie du Droit et à tous les étudiants de ma promotion. C'était fort passionnant de penser du Droit ensemble.

Enfin, je crains ne jamais avoir assez de mots pour remercier toutes ces bonnes volontés que j'ai rencontrées et qui m'ont toujours soutenu. Je pense surtout à ma mère, à mes sœurs Sophie, Emilie, Aimée, mon frère Peter et à ma fiancée Laëtitia ; à mes chers Clémence, Yves et Rodolphe et à tous mes amis.

Grand merci à tous.

Je dédie ce mémoire au Docteur Paul AMEGEE, mon père, qui n'a pas eu assez de temps pour me faire ses remarques sur ce sujet qui l'intéressait pourtant.

Papa, tu étais le meilleur

Paix à ton âme.

Si tu es prêt à sacrifier un peu de liberté pour te sentir en sécurité,
tu ne mérites ni l'une ni l'autre.

Thomas JEFFERSON

Sommaire

La cybersurveillance et le secret professionnel : paradoxes et contradictions ?

Introduction:

Annoncé comme la clé de la *« révolution technologique »* associé au nouveau millénaire, Internet pose des questions après l'engouement suscité par la nouvelle économie.
En parallèle à cette révolution technologique, l'actualité fait souvent état de l'utilisation criminelle, des nouvelles technologies. Si l'on étend le champ d'observation à l'ensemble de l'environnement électronique, l'inventaire des nouvelles formes de crimes semble illimité. Pour apprécier l'ampleur du phénomène 'cyber', il suffit de se référer aux apports décisifs des "Cybertools" aux principaux actes malveillants qui ont marqué les dernières actualités internationales.

Citons trois faits récents permettant d'illustrer le propos :

- L'explosion du blanchiment d'argent aurait-elle lieu en l'absence du progrès des nouvelles technologies de l'information et de la communication (NTIC) ?
  Plusieurs rapports venant appuyer la jurisprudence témoignent du fait que les réseaux criminels détournent les possibilités des NTIC pour parvenir à leurs fins.

- Au travers de l'affaire *« Yahoo »,* ce n'est plus seulement les auteurs des actes de nazisme ou de révisionnisme qui sont à rechercher. La cause était entendue. Il est juste question de reconnaître la nécessité de soumettre les NTIC, en dépit de leur caractère virtuel, au droit.

- Enfin, et de manière plus spectaculaire, les échanges de données via les réseaux de communication ont pu permettre d'organiser des attentats aussi gigantesques et criminels que ceux du 11 septembre 2001 aux USA.

Ainsi, le développement de l'Internet et des réseaux de communication est souvent associé à de véritables problèmes de sociétés. Dès lors, comment soumettre cette nouvelle sphère des réalités sociales à la loi sans attenter aux libertés individuelles ? Peut-on au nom d'une virtualité qui en constitue le fondement, ne pas réguler les actes liés à Internet ?

Même les adeptes du culte de la liberté totale sur Internet ont réexaminé leur position, notamment depuis les évènements du 11 septembre 2001. C'est dans cet environnement de remise en cause du 'tout libéral' du cybermonde que s'inscrivent un certain nombre de premières approches de régulation voire de législations liberticides.

Plusieurs exemples illustre cette récente inflexion de la toute puissance d'Internet face au droit :

- Le RIPA (Regulation of Investigatory Power Act) a établi une cybersurveillance sans limite en Angleterre comme mesures de police administrative.

- La loi relative à la sécurité quotidienne votée le 15 octobre 2001 consacre la cybersurveillance 'policière' en France.

- Quant à la législation américaine relative à la cybersurveillance, elle fait songer qu'on évolue vers l'abolition, non pas de la peine capitale mais du droit à la vie privée.

Mais la cybersurveillance, qu'elle soit en temps réel ou en temps différé, peut facilement porter atteinte à la vie privée des cybernautes. Il est donc de bonne augure que l'autorité judiciaire, gardienne des libertés individuelles, face preuve de vigilance envers l'autorité publique qui exerce la cybersurveillance. La Commission nationale de l'informatique et des libertés (CNIL) instituée par la loi du 6 janvier 1978, a pour rôle de contrebalancer la protection des données personnelles et les mesures de police.

Il s'agit de faire en sorte qu'aucun fait criminel ne puisse échapper à des poursuites sous prétexte de la virtualité des moyens mis en œuvre par les auteurs.

Cette tentative de régulation du cybermonde se traduit dans le domaine professionnel et dans notre champ d'études, par une législation qui n'est pas sans poser des questions.

'Officialisée' en droit français par la loi relative à la sécurité quotidienne du 15 octobre 2001, après de vives résistances des défenseurs des droits et libertés individuels, la cybersurveillance, réalise sans conteste un véritable choc des cultures. Quoi de plus incompatibles, a priori, que de trouver d'un côté, la présomption d'innocence, la liberté de communication, le droit au respect de la vie privée, le secret des correspondances, le privilège de confidentialité, le secret professionnel et de l'autre, la cybersurveillance soumise par définition à la porosité, à l'intrusion, bref, l'atteinte à la confidentialité ?

Face à un tel phénomène plusieurs questions s'imposent : la cybersurveillance remet-elle en question le secret professionnel, et dans quelles mesures ?
Aussi, voudrions-nous savoir comment concilier le nécessaire ordre public virtuel et le droit au respect de la vie privée dont le secret professionnel est l'un des garants…
Etrange équivoque que celle de la cybersurveillance dans la sphère du secret professionnel !

Après avoir analysé dans les notions de base la cybersurveillance et le secret professionnel, (Titre I), nous aborderons la cybersurveillance comme atteinte systématique au secret professionnel (Titre II). Nous traiterons enfin la question de la validité des mesures de la cybersurveillance dans la lutte contre le terrorisme, le trafic et le blanchiment (Titre III).

Titre I/ Notions de base

Dans un premier temps, nous étudierons le secret professionnel et les données personnelles (chapitre I), avant d'aborder la cybersurveillance comme mesure administrative ou judiciaire (chapitre II).

Chapitre I : Le secret professionnel et les données personnelles

Nous étudierons sous ce chapitre, tour à tour, le secret professionnel et le privilège de confidentialité (1) ; l'effectivité, la sanction et les limites du secret professionnel (2) ; la particularité du secret professionnel du journaliste (3) et le secret professionnel à l'épreuve du numérique: une nécessité de protection spécifique et une obligation de sécurité (4).

1-Le secret professionnel et le privilège de confidentialité

« Rien ne pèse tant qu'un secret »[1] : Voilà des mots qui donnent au mythe du secret tout son poids !

Que signifie 'secret' ?

Il nous semble convenable d'arpenter les méandres de l'Histoire, tout au moins remonter au XIIème siècle pour mieux appréhender le concept du secret. Le mot latin 'secretus' qui signifiait 'séparé' ou 'écarté' se trouve être l'origine du mot'secret'.

Le verbe secernere lui-même n'avait d'autre sens que " écarter ". Ainsi, le secret peut-il se définir comme quelque chose qui est hors du circuit commun. C'est une connaissance ou une information qui n'est ni connue, ni partagée ; ou alors partagée dans un cercle fermé et qui, par

[1] Jean de la Fontaine, Les Femmes et le Secret, livre VIII, Fable 6

conséquent, implique discrétion et silence.

Le petit Robert définit pour sa part le secret comme un *" ensemble de connaissances, d'informations qui doivent être réservées à quelques uns et que le détenteur ne doit pas révéler ".* D'emblée, le concept de secret recouvre deux réalités : un cercle fermé et une obligation de se taire.

L'objet du secret n'est pas accessible à tous. Les informations essentielles d'une secte ne se communiquent qu'entre adeptes. Les éléments d'une confession ne sont connus que du prêtre et du pécheur repenti. Cela renvoie imparablement à l'idée de silence. Lequel silence est sous-tendu par la confiance. L'éthique biblique ne reproche-t-elle pas à Dalila, la compagne du puissant Samson, d'avoir causé sa chute en trahissant le secret de sa force?[2] Alors, la confidence lie les parties, tel un pacte. Il faut souligner à ce niveau que la confidence, du mot latin confidentia, n'est pas synonyme du secret.

Que signifie confidence ?
La confidence n'est en réalité que la communication du secret.
La confiance est un élément déterminent, si ce n'est tout ce qui motive, celui qui confie le secret ou qui le partage dans le but de soulager sa conscience. Cette hypothèse renvoie justement à l'histoire de Raskolnikov qui n'a pu libérer sa conscience qu'en avouant son crime[3]. Mais comment se confesser si l'on n'est pas sûr que le prêtre sera discret ? Le secret fait donc corps avec la confidence et prend une dimension éthique. La garde du secret semble être un devoir moral.

Le secret du prêtre, ministre du culte, qui revêt à la fois un caractère sacré et professionnel se trouve être la loi du silence. Monseigneur Pican, évêque de Bayeux et de Lisieux, mis en accusation pour non-dénonciation de crime à caractère sexuel et pédophile en janvier 2000, alors qu'il était tenu au secret. Pouvait-il révéler les aveux reçus en confession ? Son silence peut heurter la morale commune. Celle là même qui protège le secret.

[2] Juges, La Bible de Jérusalem, chapitre 16, Les Éditions du Cerf 1997
[3] Fédor Dostoïevski, Crimes et Châtiments

L'Evangile semble lui donner bonne conscience, même si la loi et la morale de la République le condamnent : *«Plaide ta cause contre ton prochain ; mais ne révèle pas le secret d'autrui. De peur que s'il l'apprend, il ne te le reproche. Et que ta mauvaise réputation subsiste toujours»*[4]. L'ecclésiastique peut-il toujours se retrancher derrière le secret de la confession alors que des criminels eux sont toujours en liberté, jouissant d'une impunité qui ne blesse pas moins la droite raison ?

Pour la chambre criminelle de la Cour de cassation, *« cette obligation établie pour assurer la confiance nécessaire à l'exercice de certaines professions ou de certaines fonctions, s'impose aux médecins, comme un devoir de leur état ; qu'elle est générale et qu'il n'appartient à personne de s'en affranchir ».* C'est une position de principe qui s'applique au secret professionnel en général.

Ce n'est pas la Bible qui institue le secret professionnel du ministre du culte mais le droit canonique. Les canons 983 et suivants du Code de droit canonique de 1983 font du secret de confession un secret inviolable: *«Le secret sacramentel est inviolable. C'est pourquoi il est absolument interdit au confesseur de trahir en quoi que ce soit un pénitent par des paroles ou d'une autre manière et pour quelque cause que ce soit [….] L'utilisation des connaissances acquises en confession qui porte préjudice au pénitent est absolument défendue au confesseur, même si tout risque d'indiscrétion est exclu»*. L'article 35 de l'Edit de Nantes de 1598 prévoyait : *«les ministres de la religion réformée ne pourront être contraints de répondre en justice, en qualité de témoins, pour les choses qui auraient été révélées en leur Consistoire»*. Le secret est dans la présente optique donc absolu, c'est-à-dire opposable à tous, même à la justice.

Cette dimension éthique et morale n'est pas étrangère à l'honorabilité de certaines professions qui requièrent la vérité comme condition d'efficacité. D'ailleurs, le Professeur Marie-Anne FRISON-ROCHE définissait la déontologie comme un *«ensemble de prescriptions de bons comportements professionnels tels qu'on l'attend de tout bon professionnel […] c'est-à-dire une personne compétente, efficace et dans laquelle on peut avoir confiance».*

[4] La sainte Bible, Proverbe XXV, 9-10, Nouvelle Edition de Genève 1979, pp.629-659

La confidentialité constitue un abri pour la pudeur des uns et la condition même de la réussite professionnel pour les autres. La vérité du patient n'est-elle pas la condition d'un diagnostic réussi par le médecin? La confidentialité d'un dossier ne conditionne-t-elle pas le succès d'un avocat dans un procès ?

La confidence légitimée par l'éthique commune se trouve être 'la loi privée' ou 'particulière' de certaines professions : le privilège de confidentialité est la condition même du secret professionnel. Et il faut prendre privilège ici au sens étymologique : privata lex (la loi privée). Elle exonère une catégorie de personnes du fait de leurs professions de 'l'obligation de dénoncer'. En effet, le code pénal et le code de procédure pénale prévoient, dans certains cas, une obligation de dénoncer. Ainsi, l'article 434-1 du Code pénal réprime la non-dénonciation d'un crime dont il est encore possible de prévenir ou de limiter les effets, ou dont les auteurs sont susceptibles de commettre de nouveaux crimes. L'obligation ne concerne cependant ni les membres de la famille, ni les personnes astreintes au secret professionnel. Il en résulte aussi que le privilège de confidentialité constitue une fin de non recevoir à leur citation comme témoins devant une juridiction. Le privilège de confidentialité est un droit fondamental qui confirme le caractère absolu du secret professionnel. Il peut également faire échec à l'article 10 du Code civil qui oblige chacun à apporter son concours à la justice en vue de la manifestation de la vérité.
Ainsi, le professionnel a-t-il non seulement le droit mais aussi l'obligation d'opposer un refus à la divulgation du secret. Et puis, l'article 312 du Code pénal protège le secret de ces professionnels.

Il n'est pas rare qu'un avocat laisse condamner un innocent bien que persuadé de la culpabilité de son client. Le bon avocat n'est-il pas celui qui fait de son client coupable un innocent devant le juré ?
Un avocat pensait que *«le "secret professionnel" est une composante essentielle de la profession d'"avocat", puisqu'il permet au client de demander un avis juridique en étant assuré que les renseignements qu'il communique au juriste ne seront pas utilisés contre lui ».*

Le jeune avocat pénaliste, Kevin LOMAX, a défendu avec succès Alexander COLLEN, un homme violent et redoutable, accusé de meurtre sur la personne de son épouse, de son enfant et

de sa domestique. Il a plaidé non coupable, alors qu'il n'avait aucun doute de sa culpabilité, au vu des pièces à conviction à sa charge dont il avait eu connaissance. Pour plaider non coupable, un faux témoignage était nécessaire. Il a également obtenu l'acquittement d'un enseignant - un pervers sexuel - accusé d'attouchements sexuels sur une élève mineure, dont il savait la culpabilité[5]. L'avocat ne peut être poursuivi d'avoir tu un secret dans l'intérêt de son client. Voilà qui donne au privilège de confidentialité tout son sens !

La question de la protection du privilège de confidentialité s'est posée dans des actions judiciaires devant les autorités nationales chargées de la concurrence. L'avis juridique donné à un client bénéficie-t-il de la protection de la confidentialité devant les autorités nationales chargées de la concurrence ou, au contraire, peut-il être utilisé par ces autorités contre le client, personne morale ou physique, concerné ? La plupart des Etats de l'Union européenne admettent que les avocats externes peuvent invoquer l'obligation de secret professionnel pour refuser de témoigner devant le Conseil de la Concurrence.

Un avocat français peut-il invoquer la confidentialité pour les avis qu'il donne à ses clients, même devant la Direction Générale de la Concurrence et de la Consommation ? En effet, un arrêt du 30 septembre 1991 de la Cour de Cassation a introduit une distinction entre les avis donnés par un avocat dans sa mission de défense et dans sa fonction de conseil. La haute juridiction a jugé que seuls les défenseurs sont protégés par le secret professionnel dans les affaires criminelles.

« L'effet de cet arrêt (Cour de cassation 30 septembre 1991) sur les avis donnés dans des affaires relatives au droit de la concurrence n'est pas encore clairement établi. Dans tous les cas, il n'existe pas de dispositions particulières régissant les affaires en matière de droit de la concurrence. Le juriste d'entreprise ne bénéficie pas du secret professionnel en général et ne devrait donc pas pouvoir l'invoquer devant les autorités chargées de la concurrence »[6].

[5] Hackford Taylor, l'associé du diable, livre aux éditions Pocket ; film Warner Bros, USA - 1997

[6] La protection de la confidentialité (*legal privilege*) dans les actions judiciaires devant les autorités nationales chargées de la concurrence, http://www.ecla.org/fr/objectifs/nationales.htm

Le secret professionnel selon le petit Robert est *" l'obligation de ne pas divulguer des faits confidentiels appris dans l'exercice de la profession, hors des cas prévus par la loi"*. Le secret professionnel est la transposition du secret au sens commun dans le cadre professionnel où il est érigé en norme. Le secret est une règle déontologique. Ses origines en faisaient presque le résumé du secret médical (voir l'article 378 de l'ancien Code pénal).

Qu'est le secret médical ?

Alain Bensoussan estime que *« la notion de secret médical est née du colloque singulier qui s'instaure entre le médecin et son patient dans le secret de son cabinet »*[7].
En effet, si l'on admet que le cabinet médical est le lieu officiel ou du moins propice pour l'exercice de la profession médicale, on peut accepter ce point de vue.

Cependant, force est de contacter que le médecin opère également en dehors de son cabinet sans que pour autant sa mission puisse changer. Les médecins du SAMUS, SOS médecin...bref, tous ces médecins ambulants qui soignent volontiers le patient chez lui. 'L'hospitalisation à domicile', vieille pratique, est plus que jamais d'actualité. Les informations tirées de cette mission tombent aussi sous le coup du secret médical.

Est-ce pour cela que le Professeur Louis PORTES, Président du Conseil National de l'Ordre des médecins à l'académie des sciences morales et politiques, déclarait le 5 juin 1950 qu' *« il n'y a pas de médecine sans confiance, de confiance sans confidence et de confidence sans secret »* ?

Comment soigner efficacement sans faire immixtion dans la vie privée, dans l'intimité même du patient?

Autrefois, au temps d'Hippocrate, le médecin était cette personne à qui l'on reconnaissait, nollens, vollens, le droit de "violer" l'intimité de la vie familiale. Ce n'est qu'en rentrant dans le cercle protégé de la vie privée que le médecin effectue un diagnostic efficace. Il faut reconnaître

[7] Alain Bensoussan, *Informatique et télécoms,* éd. Francis Lefebvre, 1997, p. 564 et 565,895

qu'entre vie privée et vie 'tout court', le choix est vite fait. Plutôt souffrir de la violation de la vie privée que mourir dans le secret de son malaise [8] : n'est-ce pas la devise des patients ?

En outre, le respect de la vie privée est non seulement une exigence morale mais aussi une exigence légale. L'article 9 du Code civil à cet égard est clair: *"Chacun a droit au respect de sa vie privée"*. Le droit au respect de la vie privée est universellement reconnu: *"Nul ne sera l'objet d'immixtions arbitraires dans sa vie privée..."* (Article 12 de la Déclaration universelle des droits de l'Homme). Le respect de la vie privée est un impératif catégorique. Si atteinte il doit y avoir à la vie privée, cette atteinte doit être légitime ; c'est-à-dire fondé en droit. L'accès au soin doit être doublement perçu à cet effet. Il s'agit d'accéder au soin en tant que donneur de soins mais aussi en tant que bénéficiaire de soins.

Dès lors, le secret médical apparaît comme un impératif catégorique. Il est hors de question que le médecin puisse révéler ce qu'il aurait découvert chez le patient à un tiers. Dès lors, il convient plutôt de penser que le secret médical naît du contact, de la relation entre le médecin et son patient.

Jules Barbe d'Aurillac pensait que *" le médecin est obligé au secret de la confession comme le prêtre "*. Le secret professionnel dans cette optique semble revêtir à la fois d'un caractère normatif mais aussi sacré ou, du moins, moral.

"Les choses que je verrai ou que j'entendrai dire dans l'exercice de mon art, ou lors de mes fonctions dans le commerce des hommes, et qui ne devront pas être divulguées, je les tairai, les regardant comme des secrets inviolables." : ce passage du serment d'Hippocrate fait du secret médical un impérieux devoir pour le médecin.

Un médecin, et particulièrement un psychiatre, ne peut se voir reprocher de ne pas révéler à la police l'état psychique dangereux de son patient. Les voix se sont élevées contre le silence du psychiatre de Ricard DURN qui eût empêché que ce dernier fût libre et hors de tout soupçon. La scène d'horreur, quelque peu prévisible, a eu lieu. Il est alors impossible de poursuivre le

[8] Parodie de *" plutôt souffrir que mourir : c'est la devise des hommes ",* De LAFONTAINE J.

psychiatre de Richard DURN[9] de ne pas avoir prévenu la police des intentions meurtrières de son patient. Dans la pensée du professeur Marie-Anne FRISON-ROCHE, *« ce qu'il est convenu d'appeler le secret professionnel est un beau sujet de réflexion pour le juriste et pour le moraliste, car cette notion doit s'efforcer de concilier tant le droit que la morale. Si la défense des biens et la protection de la personne physique ne posent guère de problèmes, il n'en va pas de même lorsqu'il s'agit de préserver l'individu de toute intrusion abusive dans l'intimité de sa vie privée, d'autant plus si l'auteur de l'atteinte est précisément le confident auquel la personne s'est adressée parce qu'elle le considérait comme un confident nécessaire, et comme le seul confident possible ».*

En outre, le secret professionnel constitue un élément fondamental des droits de la défense.

Émile Garçon, dans son commentaire de l'article 378 du code pénal, écrivait: *" Le bon fonctionnement de la société veut que le malade trouve un médecin, le plaideur un défenseur, le catholique un confesseur, mais ni le médecin, ni l'avocat, ni le prêtre ne pourraient accomplir leur mission si les confidences qui leur sont faites n'étaient assurées d'un secret inviolable.*

Il importe donc que ces confidents nécessaires soient astreints à la discrétion et que le silence leur soit imposé sans condition ni réserve, car personne n'oserait plus s'adresser à eux si l'on pouvait craindre la divulgation du secret confié. Ce secret est donc absolu et d'ordre public ".

A l'ouverture du colloque *" Le secret professionnel ",*organisé par la Conférence des bâtonniers à l'Assemblée nationale le mercredi 22 novembre 2000, Raymond FORNI, Président de l'Assemblée nationale, ajoutait pour sa part qu' *« il n'y a pas de défense, si une part de secret n'est pas maintenu : secret sur l'état de santé de tel ou tel, secret des pensées et des penchants dans la confession, secret des lettres, correspondances et confidences entre un avocat et son client. Le secret est d'abord un contre-pouvoir. Il est l'espace qui résiste à l'investigation du public. Il est la part qui protège du regard inquisiteur de la société. En deuxième lieu, le secret est l'élément central du principe de confiance légitime parce qu'il n'y*

[9] Mercredi 27 mars 2002 Richard Durn tue huit conseillers municipaux de Nanterre. L'assassin avait un dossier psychiatrique qui témoignait de sa dangerosité. http://www.liberation.fr/quotidien/portrait

a pas de défense possible si celui à qui je me confie me trahit, livre mes secrets à mon adversaire ou à l'accusation ! »

La sanction, quant à elle, est la garantie même de la force obligatoire d'une norme.

Le non respect du secret professionnel est sanctionné par l'article 378 du Code pénal, devenu article 226-13 dans le Nouveau code pénal de 1992. Il impose aux membres de certaines professions, à l'instar du prêtre, de ne pas divulguer les informations connues dans le cadre de leurs professions. Lors de sa rédaction, cet article du Code pénal visait le prêtre, le médecin et l'avocat. *« On s'aperçut par la suite que l'article 378 était incomplet : on avait oublié les magistrats et les jurés »*[10].

Le domaine du secret professionnel est désormais vaste. Il couvre aussi bien les milieux d'affaires, notamment bancaires où l'on confie son patrimoine[11], que le cadre social ou ordinal traditionnel.

La sanction du secret professionnel par le Code pénal est la condition de son effectivité. Cependant, la répression de la violation du secret et l'exception au respect du secret vont de concert.

Il convient, dès lors, de se pencher sur la validité du secret professionnel en tant que norme.

2-<u>L'effectivité, la sanction et les limites du secret professionnel</u>

L'effectivité d'une norme relève d'une question essentielle qui est la validité de la norme. Mais il suffit d'aborder la question de la validité pour s'apercevoir que le positivisme n'est pas ce

[10] Le secret professionnel in Encyclopoedia universalis 1990, Encyclopoedia universalis France éditeur à Paris, p. 3170

[11] Il faut garder à l'esprit que les banquiers sont également soumis au secret professionnel, Cour d'Appel de Paris, 6 février 1975, D 1975, p. 318, note Vézian.

courant continu et homogène. Kelsen a montré que la théorie du droit n'a jamais cessé d'osciller entre deux positions extrêmes. Il y a d'un côté la conception idéaliste[12] et de l'autre côté la conception réaliste[13].

La norme valide, selon la conception réaliste, n'est pas une prescription observable mais une prescription effectivement observée. Il faudra en déduire que les commandements qui ne sont pas effectivement obéis ne constituent pas des normes valides. La validité renvoie ainsi à l'effectivité. Kelsen estime que dans cette optique le droit n'est plus un monde du devoir être " sollen " mais un monde de l'être " sein". *" La norme valide peut se définir comme un ensemble de règles qui régissent effectivement les rapports sociaux "*.
Pour Kelsen, la validité d'une norme qui vient d'entrer en vigueur qui n'a pas encore été appliquée par les tribunaux ne fait aucun doute. Il distingue donc *validité* et *effectivité*[14].

Dans la conception de Ross[15], la norme est considérée comme valide que si elle est réellement obéie par ceux qui y sont assujettis. En effet, le droit est un ordre, une contrainte. Par conséquent, la norme valide est la norme efficace. Enfin, dans la conception de Ross, une norme est valide si elle est ressentie comme socialement obligatoire.

A la lumière de cette conception réaliste, le secret est aussi une obligation déontologique et légale, pénalement sanctionné. Le secret professionnel est une obligation de discrétion et un privilège de confidentialité réellement protégés par un système juridique. Seule l'observation de l'obligation au secret (posée en tant que norme pour les professionnels) assortie d'une sanction constitue la base de l'effectivité du secret professionnel.

Le professionnel astreint au secret est effectivement tenu à un devoir de discrétion. Du moins, il

[12] La conception idéaliste de la validité qui est la conformité à un idéal. La norme correspond à un paradigme, d'où la thèse de présupposé. Dès lors, l'existence de la norme en tant que telle entraîne sa validité. La validité est dans cette optique la signification objective de la norme. A cet égard, l'idéalisme ne fait aucune distinction entre la validité et la juridicité d'une prescription.

[13] La conception réaliste de la validité renvoie à l'effectivité qui est le caractère obligatoire de la norme.

[14] Hans KELSEN, *Théorie pure du droit*, traduit par Charles Eisenmann, LGDJ, 1999 p.367

[15] Alf ROSS, *On Justice and Law* : la validité matérielle de la norme est son efficacité.

ne saurait révéler, de son propre chef, les informations connues dans le cadre de sa profession, au risque d'une peine d'emprisonnement et d'une amende prévues par la loi. C'est précisément ce que pensait Kelsen. Pour ce dernier la norme est valide dès lors que sa violation est sanctionnée. Kelsen, comme John Austin, semblent partager que la détermination de la sanction constitue l'essence même du droit, même si Hart reprochait à Kelsen de réduire le droit à des *« règles primaires »* assorties de sanctions.

Il semble aller de soi que le *« devoir être »* n'existe vraiment que si le *« non-être »* (qui s'y rapporte) est sanctionné. Le caractère obligatoire de la norme n'est pas analogue à celui d'une règle morale. Par exemple, le fait de dévoiler une confidence faite en privé, en dehors de toute hypothèse de secret professionnel, heurte la morale comme nous l'évoquions supra. Mais le simple fait de trahir la confiance d'un confident n'est pas puni par la loi. Cependant l'avocat qui révèle le contenu du dossier de son client risque de subir, réellement, une peine d'un an d'emprisonnement et de 15244,90 Euros en vertu de l'article 226-13 du Nouveau Code Pénal. Par conséquent, la validité de la norme est une menace autoritaire fondé sur un pouvoir exorbitant de droit commun.

Du moment où la norme constitue une épée de Damoclès sur la tête du sujet, la précision de la loi serait une garantie nécessaire contre l'arbitraire. A cet égard la maxime latine *«nullum crimen, nulla poena sine lege »*, il n'y a ni crime ni peine sans loi, mérite de l'attention. Cet adage représente le principe fondamental du droit pénal qu'est la légalité des délits et des peines prévue par article 11 du Code pénal (111-3 du Nouveau Code pénal). L'article 11 du Code pénal n'en était finalement que la juste transposition. De plus, ce principe est une garantie de poids. Il a une valeur constitutionnelle et a été consacré par l'article 7 de la Déclaration des droits de l'homme et du citoyen du 26 août 1789.

En revanche, le législateur ne peut tout dire. Le rôle de la jurisprudence dans l'édiction de la norme est parfois prépondérant. Dans *Les archives de philosophie du droit*, le professeur Michel TROPER pensait que *« l'interprétation consiste à déterminer la signification qu'un énoncé est supposé exprimer. La signification de la loi est donc déterminée par le juge, qui, en tant qu'interprète, devient le véritable auteur de la loi ».* Alexandre Viala pensait pour sa part que le

juge ordinaire en interprétant la loi *« s'arroge indûment le pouvoir de colégislation »*.[16] La connotation médicale de l'article 378 de l'ancien Code pénal[17] n'a pas empêché le juge de préciser et d'élargir le domaine du secret professionnel partout où le besoin s'en ressent. Portalis disait à juste titre que *« le juge est maître de la loi quand le législateur a parlé »*.

Il faut inscrire dans une parenthèse que pour ce qui concerne le secret professionnel le caractère évolutif du droit semble très perceptible. L'évolution des rapports sociaux est prise en compte et le législateur de 1992 s'est gardé de désigner nommément les professionnels astreints au secret.

L'article 226-13 du Nouveau Code pénal (ex-article 378 du Code pénal) dispose : *« la révélation d'une information à caractère secret par une personne qui en est dépositaire soit par état ou par profession, soit en raison d'une fonction ou d'une mission temporaire, est punie d'un an d'emprisonnement et de 100 000 F (soit 15244,90 Euros) »*.
Force est de constater que la marge de manœuvre laissée au juge dans son interprétation est nettement plus grande. Le juge apprécie et décide souverainement que telle ou telle catégorie de professionnels est soumise au secret professionnel. Une partie de la doctrine semblait se méfier des aléas judiciaires à ce sujet. Rappelons-nous qu'on a pu parler de *« loto du secret professionnel »*[18].

Ainsi, l'avocat, le notaire, l'expert-comptable, le banquier, le médecin, l'assistante sociale, le ministre du culte, pour ne citer que ceux-là, sont-ils soumis à la même règle (sous peine d'une amende et d'un emprisonnement): le secret professionnel.

Dans l'hypothèse du secret médical, la jurisprudence semble controversée. Mais qu'en est-il

---

[16] Alexandre VIALA, *Maître de Conférences de droit public à l'Université Pierre Mendès France, Grenoble II,* L'interprétation du juge dans la hiérarchie des normes et des organes, http://www.conseil-constitutionnel.fr/cahiers/ccc6/viala.htm

[17] L'article 378 de l'ancien Code pénal disposait que *" les médecins, chirurgiens et autres officiers de la santé, ainsi que le pharmacie, les sages-femmes et toutes autres personnes dépositaires, par état ou par profession ou par fonctions temporaires ou permanentes, des secrets qu'on leur confie, qui, hors le cas où la loi les oblige ou les autorise à se porter dénonciateurs, auront révélé ces secrets, seront punis d'un emprisonnement de six mois et d'une amende de 500F à 15 000F "*.

[18] Patrick NICOLEAU, *Lexique de droit privé*, ellipses, 1996, pp.316-317

réellement ?

Paul MONZEIN pensait que *« pour que le secret soit violé, il faut qu'il soit diffusé à une tierce personne. Entre le médecin et le malade il ne peut y avoir de secret »*[19]. Il convient donc d'écarter les révélations faites par le médecin au patient, après examens et diagnostic, sur son état de santé etc. En revanche, la situation se renverse avec la qualité des interlocuteurs et non avec la quantité de l'information divulguée.

Dans un arrêt du 30 avril 1990, la Cour d'appel de Versailles a jugé que l'infraction est constituée même en cas de révélation partielle. Même si cette révélation n'a pas causé de préjudice. Il est indifférent que le fait révélé par le médecin puisse être connu en en l'absence de cette révélation[20]. A fortiori, le caractère général et absolu du secret médical a pour conséquence l'impossibilité pour le médecin d'en être libéré en dehors des hypothèses prévues par la loi. Le médecin ne peut même pas se prévaloir de la permission du patient pour révéler des faits qui tombent sous le secret professionnel. Tel était la position de la Cour de cassation dans un arrêt du 18 mars 1986[21]. Dix ans plus tard, presque jour pour jour, la Cour d'appel de Paris rejetait dans un arrêt du 13 mars 1996 l'argument du Docteur Gubler selon lequel le Président Mitterrand l'avait autorisé de son vivant à publier ses bulletins de santé[22]. Le secret professionnel fait figure d'une obligation générale est absolue. C'est-à-dire qu'il est opposable à tous, y compris le patient[23]lui-même lorsque le médecin en juge ainsi, s'appuyant sur de raisons légitimes.

Madame le substitut Général B. Girardin a souligné dans ses observations sur l''affaire Gubler' que le secret professionnel est d'ordre public, que sa violation trouble l'ordre public et engage la responsabilité civile de celui qui contrevient à ce secret[24]. Même si Madame Girardin s'est prononcée dans l'hypothèse du secret médical, il faut remarquer qu'elle s'est prononcée en faveur du secret professionnel dont la force obligatoire se trouve ainsi, encore une fois, réaffirmée.

---

[19] Paul Monzein, *Réflexion sur le secret médical*, D.1984, chron. P.9
[20] CA Versailles 30 avril1990 : D.1990 IR, p. 178
[21] Cass. 1e civ. 18 mars 1986 : JCP éd. G 1986 II n°20629
[22] CA 1e ch. 13 mars 1996, Sté Ed. Plon et autres c/ Cts Mitterrand et autres : JCP éd. G 1996 II n° 22632
[23] Article 35 al. 2 et 3 du Code de déontologie médicale
[24] Ibid., 22

" Le silence quand-même et toujours ", disait le docteur BRAOUARDEL. Son approche du secret médical, moins absolue que celle de MUTEAU[25] au XIX[e] siècle, est fort édifiante[26].La Chambre criminelle de la Cour de cassation a consacré la thèse de MUTEAU dans l'affaire Watelet le 18 décembre 1885. Il s'agissait en l'espèce d'une poursuite dirigée contre un médecin qui a violé, malgré lui, un secret médical.[27]

Le Docteur WATELET a soigné avec d'autres médecins, un peintre réputé Bastien LEPAGE. Celui-ci a présenté un cancer du testicule et, sans espoir de le sauver, ses médecins l'ont autorisé à faire un dernier voyage en Algérie « pour convalescence ». A sa mort, une campagne de presse se déclenche contre WATELET, l'accusant d'avoir négligé de traiter une maladie vénérienne chez l'illustre patient. Pour se défendre contre la calomnie, le médecin adresse au journal Le Matin, une lettre par laquelle il rétablit, en révélant la vraie nature de la maladie du peintre. Il est alors poursuivi par le Parquet pour avoir enfreint l'article 378 du Code Pénal d'alors et condamné en première instance, puis en appel. S'étant pourvu en cassation, il suscite un arrêt de la Cour de cassation du 18 décembre 1885 qui rejette son pourvoi en précisant dans ses attendus que la disposition de l'article 378 *« est générale et absolue et qu'elle punit toute révélation du secret professionnel sans qu'il soit nécessaire d'établir à la charge du révélateur l'intention de nuire ».*

Cependant, la règle du secret souffre quelques exceptions pratiques et légales qui en sont des limites : le secret partagé et la dénonciation.

- Le secret partagé

Le secret est *partagé* lorsque les professionnels sont amenés à se communiquer, en équipe, des informations relevant du secret professionnel. Il en va souvent dans l'intérêt du patient d'être prise en charge par une équipe pluridisciplinaire. Dans ce cas une conception trop stricte du

---

[25] MUTEAU Ch., *Du secret professionnel, de son étendue et de la responsabilité qu'il entraîne*, Paris 1870
Dans la conception de MUTEAU, le secret professionnel est absolu. Seule la conscience du professionnel guidera son choix de divulguer ou non le secret.

[26]Docteur BRAOUARDEL P., *Le secret médical*, Baillière, Paris, 2[e] éd., 1993

[27] Crim., 19 décembre 1885, aff. Watelet, S., 1886, I. 176, rapport Tanon, D.188.I347.

secret professionnel serait une entrave à la pratique. Cela rappelle la formule d'Alexis De TOCQUEVILLE dans *l'Ancien Régime et la Révolution* : *« Une règle rigide, une pratique molle ».*

A contrario, une pratique efficace nécessite un assouplissement de la règle. Au sein d'un cabinet d'avocats, force est de constater que la collaboration n'a de sens que si les partenaires accèdent aux dossiers qui constituent le puits du secret.

Enfin, sans que la liste soit exhaustive, les employés d'une même agence bancaire gèrent le plus souvent, tour à tour, l'ensemble des dossiers des clients. Ils partagent ainsi le secret bancaire. La garantie de la confidentialité réside dans la soumission de toute une équipe ou tout un cabinet au secret professionnel. C'est dans cette optique que tout le personnel de tout un cabinet est soumis au secret professionnel. (Ce n'est pas pour autant que les salariés vont prêter serment de confidentialité.). En effet, par un arrêt du 19 octobre 1994, la chambre sociale de la Haute juridiction l'a bien précisé : *« une salariée tenue par ses fonctions au secret professionnel n'a aucune obligation de faire le serment de confidentialité à son employeur et qui présente un caractère superfétatoire, vexatoire et désobligeant »*[28].

Que tirer comme conclusion ? La confiance qui sous-tend le secret professionnel serait-elle chose librement partagée ?

Il en ressort, tout de même, que le secret professionnel ne relève, ni de la compétence, ni de la volonté de l'employeur. Le secret professionnel relève en principe de la compétence législative. Tel est du moins le sens formel de l'article 226-13 du Nouveau Code pénal (NCP).

Toutefois, le 'secret partagé' n'est pas prévu par la réglementation du secret professionnel. Est-ce une preuve que le législateur pencherait plus du côté de la conception absolue du secret professionnel ?

[28] Cass. Soc. 19 octobre 1994, n°3759D.

Dans un rapport d'une session du Conseil National de l'Ordre des Médecins[29], docteur Aline MARCELLI écrivait à cet sujet : *« Le 'secret partagé' n'a aucune base légale ou réglementaire et s'oppose au caractère général et absolu du secret médical. Mais le partage de l'information entre professionnels de santé s'est imposé, au cours des siècles, dans la pratique quotidienne, afin d'assurer la continuité des soins et d'améliorer leur qualité dans l'intérêt des patients. L'exercice pluridisciplinaire a accentué cette tendance ».*

Les professionnels astreints au secret disposent également de la faculté de *se porter dénonciateurs.* Si les personnes tenues au secret professionnel n'ont pas l'obligation de dénoncer un délit, elles peuvent toutefois le faire après avoir été déliées du secret par l'autorité compétente. Il existe également des hypothèses où les professionnels sont obligés de dénoncer un délit ou divulguer un secret professionnel. Il convient que l'on s'y arrête pour en saisir le sens et la portée.

- La dénonciation

D'une part, l'article 226-14 du Nouveau Code pénal prévoit des cas où le professionnel est exonéré de l'obligation au secret. En vertu de cet article, l'obligation au secret ne s'applique pas : *« à celui qui informe les autorités judiciaires, médicales ou administratives (L. n°98-468 du 17 juin 1998) de sévices ou privation dont il a eu connaissance et qui ont été infligés à un mineur de quinze ans ou à une personne qui n'est pas en mesure de se protéger en raison de son âge ou de son état physique ou psychique »* ; il ne s'applique pas non plus *« au médecin qui, avec l'accord de la victime, porte à la connaissance du procureur de la République les sévices qu'il a constatés dans l'exercice de sa profession et qui lui permettent de présumer que des violences sexuelles de toute nature ont été commises ».*

A la lecture de ces deux alinéas de l'article 226-14 du Nouveau Code pénal, on peut conclure que cette dérogation concerne notamment les sévices contre mineurs de quinze ans ou personnes vulnérables (en raison de l'âge, l'état physique ou psychique…) et de violences

[29] Le rapport de la session de mai 1998 du Conseil National de l'Ordre des Médecins, *Le secret partagé*, réf : http://www.conseil-national.medecin.fr/CNOM/Home.nsf/vPages/references?OpenDocument

sexuelles. Par conséquent, les sévices pratiqués sur les mineurs doivent eux aussi pouvoir être révélés sans risque de poursuite pénale.

« Violences sexuelles de toute nature » ne signifie pas forcément viol. La tentative de viol ou toute autre forme d'agression sexuelle peut justifier le bris du secret professionnel. Dans ces cas, le médecin peut révéler les informations tirées de ses diagnostics ou de la confidence du patient sans tomber sous le coup de l'article 226-13 du Nouveau Code pénal. D'autre part, le problème des avortements clandestins a mis en évidence le fait que les médecins et auxiliaires médicaux devaient, pour aider la justice, être affranchis de leur obligation.

Mais cette faculté de se porter dénonciateur est une obligation pour les médecins départementaux de protection maternelle infantile (PMI) en vertu de l'article 434-3 al. 2 du Nouveau Code pénal[30]. A ce sujet, le juge dispose également d'un pouvoir discrétionnaire d'appréciation.

Ainsi, l'exception de sécurité publique justifie-t-elle le bris du secret professionnel. La Cour suprême du Canada a établi récemment qu'un psychiatre de Vancouver avait le droit de révéler à la cour les confidences d'un de ses patients en passe de devenir un prédateur sexuel et un tueur en série.

L'arrêt rendu dans l'affaire Jones c. Smith[31] par la Cour suprême du Canada qui découle de faits relativement simples en témoigne amplement. L'avocat d'une personne inculpée d'agression sexuelle fait appel à un psychiatre pour l'aider à préparer la défense de l'accusé. Ce dernier a accepté de se soumettre à l'examen et a confié au médecin des informations indiquant qu'il constituait un danger permanent pour la société. Parce que, tant que l'accusé serait en liberté, il commettrait d'autres crimes violents contre des femmes. Seul un traitement approprié l'empêcherait de récidiver.

[30] Article 434-3, al.2 du Nouveau Code pénal : " sont exceptées (de l'obligation de dénoncer les sévices infligés aux mineurs de quinze ans ou aux personnes vulnérables) les personnes astreintes au secret dans les conditions prévues par l'article 226-13 ".
[31] Un arrêt rendu par la Cour suprême du Canada le 25 mars 1999 sous no du greffe: 26500.
Consultable sous http://www.bibl.ulaval.ca/info/ajour/ajour59.html

L'accusé ayant plaidé coupable, le psychiatre a informé l'avocat de ses inquiétudes mais a appris que son rapport ne serait pas pris en compte à l'audience de détermination de la sentence. C'est alors que le psychiatre s'est adressé aux tribunaux pour faire déclarer qu'il avait le droit de divulguer les renseignements qu'il détenait et qui étaient manifestement l'objet d'une obligation de confidentialité dont il n'avait pas été relevé. La question posée était d'autant complexe que le rapport du psychiatre avait été nécessaire à l'avocat de l'accusé. Le secret professionnel de l'avocat était également en cause puisque c'était lui qui avait requis l'opinion du médecin.

L'arrêt de la Cour suprême porte donc, au premier chef, sur la levée du secret professionnel de l'avocat mais, par le fait même, il indique dans quelles circonstances le psychiatre pouvait informer les autorités policières des craintes suscitées par son entrevue avec l'accusé.

D'autre part, en dehors de la démarche spontanée et libre du professionnel que celle de se porter dénonciateur ou informateur, le professionnel peut être contraint de divulguer le secret.
Autant, l'article 226-13 du Nouveau Code pénal fait de la violation du secret professionnel un délit pénal, autant le refus de témoigner constitue une infraction en vertu de l'article 109 du Code de procédure pénale : paradoxe ou contradiction ?

Face à ce dilemme, le professeur Jean PRADEL envisage *« deux attitudes possibles : ou bien le secret professionnel l'emporte et constitue un fait justificatif du refus de témoigner, ou bien, au contraire, l'obligation de témoigner s'impose et joue comme fait justificatif de la violation du secret professionnel »*[32]. Le témoignage en dépit de l'obligation au secret professionnel s'inscrit la thèse du secret professionnel relatif. On peut se référer à l'analyse de FLORIOT à cet égard.[33] La querelle doctrinale autour du caractère du secret professionnel ne s'arrête pas là.

Des commentaires font souvent état d'opposition entre la doctrine de la Chambre criminelle de la Cour de cassation et la doctrine des chambres civiles. La doctrine de la Chambre criminelle reposerait sur une conception absolue du secret professionnel alors que pour les chambres civiles

[32] Jean PRADEL, Procédure pénale, Cujas, 10e éd., 2000/2001, pp.361-363
[33] R. FLORIOT et R. COMBALDIEU, Le secret professionnel, Flammarion, 1973

il serait relatif. La conception absolue du secret médical qu'à la Chambre criminelle explique qu'elle puisse aller à l'encontre de la manifestation de la vérité devant une cour d'assise. On citera un arrêt du 16 décembre 1992[34]. En l'espèce, la Chambre criminelle a admis qu'un médecin qui avait examiné une mineure victime d'un viol était libre de refuser de témoigner et de révéler le diagnostic qu'il a porté et les médicaments qu'il a prescrits.

Il y a lieu de soulever un paradoxe au regard de l'article 4 du Code de Déontologie du décret n°95-1000 du 6 septembre 1995[35]. Cet article prévoit que « le secret professionnel, institué dans l'intérêt des patients, s'impose à tout médecin dans les conditions établies par la loi. Le secret couvre tout ce qui est venu à la connaissance du médecin dans l'exercice de sa profession, c'est à dire non seulement ce qui lui a été confié, mais aussi ce qu'il a vu, entendu ou compris ».
Une déduction s'impose à cet égard, le patient dans l'intérêt duquel le secret est institué est donc maître du secret. Peut-il alors, à souhait, en autoriser ou en exiger la divulgation?

Il ressort amplement de l'arrêt du 16 décembre 1992 (évoqué supra) que même le patient dans l'intérêt duquel le secret est institué ne peut ne peut obliger le médecin à le divulguer. Si l'on admet que le professionnel n'est pas lié par la volonté du maître du secret (le client ou le patient) alors on peut conclure que le secret professionnel revêt d'un caractère général et absolu.

Toutefois, dans le cadre du secret médical, des assouplissements méritent d'être notés. On signalera d'abord l'article 76 du Code de déontologie médicale qui autorise le médecin à délivrer au patient, sur sa demande un certificat médical. Le certificat médical n'est en réalité que l'expression d'un diagnostic qui peut être indifféremment positif ou négatif. Le cas contraire nous placerait dans l'hypothèse d'un certificat de complaisance qui relèverait du délit du faux prévu par l'article 441-1 du Nouveau Code Pénal[36]. La Chambre criminelle a appliqué l'article 76 du Code de la déontologie médicale dans un arrêt un arrêt du 5 novembre 1981[37]. En l'espèce la Haute juridiction a jugé que le versement au débat d'un certificat médical par le patient lui-même ne constitue pas une violation du secret médical.

[34] Cass. crim., 16 déc1992, n°90-86.385 Bull. crim. n° 424, p. 1189
[35] J.O. 8 septembre 1995 p. 13305
[36] Ce serait le faux intellectuel: l'acte est valable quant à la forme mais le contenu est faux.
[37] Cass. crim., n°81-90.488, Bull crim. n°190, p.481

Dans la pratique, il est rare qu'un médecin refuse de délivrer un certificat à son patient. Nonobstant, le certificat médical ne doit jamais être fourni à un tiers (ami, voisin, adversaire, administration ou compagnie d'assurance[38] et ne saurait contenir un détail sur l'état de santé du patient. C'est ce qu'énonçait la première Chambre civile dans un arrêt du 18 mars 1986 : *« le secret médical doit être observé à l'égard des tiers, en particulier quand ils en demandent la révélation par l'intermédiaire du malade lui-même »*[39].

Songeons aussi au droit, récemment consacré, du malade à la consultation de son dossier médical, qui n'est pas sans poser problème dans certains cas. Pensons également au débat passionné sur l'accouchement sous " x " et sur le droit pour chacun de nous de connaître ses origines. C'est bien dans les ères du secret médical que le particulier vient chercher des informations partagées entre deux volontés contradictoires : celle d'une mère qui veut jouir de son anonymat et celle d'une vie qui cherche un repère.

Par ailleurs, à la fin du XIX^{e} siècle, en marge de la jurisprudence de la Cour de cassation, G. LE POITTEVIN pensait que le secret professionnel disparaît dans l'accord de la personne qui a intérêt à ce qu'il soit gardé.[40] PLANIOL quant à lui soumet le secret aux besoins de la procédure judiciaire et administrative.[41] La théorie du 'conflit des devoirs' développée au début du siècle dernier par ROUX confie à la loi la charge de résoudre le dilemme du secret professionnel et de l'obligation de déposer. Seule la loi dira lequel des deux devoirs en conflit doit l'emporter.[42]

D'un côté, il y a le secret professionnel qui est *« d'ordre public »*[43] qui sous-entend une idée d'intérêt général. Lequel intérêt général réside dans le concept même du secret professionnel. D'un autre côté, il y a l'intérêt général de la Justice (la décision éclairée, juste et équitable). Que choisir ?

---

[38] Ordre national des médecins, Commentaires du Code de déontologie médicale, 1996, pp. 53-255
[39] Cass. 1re civ. 18 mars 1986, n°84-15.702, n°165, Bull.civ. I, p.196
[40] G. LE POITTEVIN, note au S., 1897.I.81, sous Req. 9 avril 1895.
[41] M. PLANIOL, note au D., 1899.I.585, sous Civ., 1er mai1899
[42] J.A. ROUX, note au S., 1914.I.169, sous Crim., 9mai 1913
[43] Madame le substitut Général B. Girardin (déjà citée),
CA 1^{e} ch. 13 mars 1996, Sté Ed. Plon et autres c/ Cts Mitterrand et autres : JCP éd. G 1996 II n° 22632

On peut convenir avec J.-P. SARTRE que *« se taire c'est être complice ».* Mais la pensée de Montesquieu peut être prise pour le compte des concepts en conflit : *« Une injustice faite à un seul est une menace faite à tous ».* Il n'est peut-être pas juste de trahir un secret mais il est tout autant injuste de se taire lorsque 'parler' devient un devoir. Que faire lorsque le renseignement enfoui sous le poids du secret devient un devoir moral?

Seule la loi libèrerait définitivement la conscience dans un tel cas. On peut d'ores et déjà se référer à la loi dite « Loi sécurité quotidienne » du 15 octobre 2001. Celle-ci institue l'obligation de remettre les clefs de chiffrement à la justice sur sa demande.

Quel que soit l'objet du secret et quel que soit le statut du professionnel concerné, et sauf circonstances exceptionnelles, celui-ci ne peut se dégager, seul, de la charge du secret. Si des situations exceptionnelles libèrent de la prescription de l'article 226-13 NCP, il est possible de conclure que le secret professionnel n'est pas forcément absolu. En définitive, la divulgation du secret ne constitue un délit que si elle est délibérée.

Dès lors, l'idée d'un secret professionnel du journaliste suscite quelques interrogations. Parce que le journalisme se trouve être la profession type de la liberté d'expression. Cela semble un peu paradoxal. Le secret professionnel du journaliste serait-il un cas particulier ? Il convient, pour ce faire, de le traiter en marge.

3- <u>La particularité du secret professionnel du journaliste</u>

S'il y a une profession à laquelle le secret professionnel ne semble pas du tout applicable, parce que difficilement concevable, ce serait bien le journalisme. Secret et liberté d'expression ne sont-ils pas, a priori, deux concepts contradictoires, irréductiblement contradictoires ?

Le métier du journaliste consiste à divulguer des informations c'est-à-dire à rendre publics des faits dont il a connaissance et qui, a priori, n'est pas connu de tous. Quel intérêt d'appendre des nouvelles déjà connues ? D'ailleurs, peut-on encore dire 'nouvelles' lorsque les faits ou événements publiés sont déjà connus ? Le 'secret' ne constitue-t-il pas l'appas essentiel du journaliste en quête d'un auditoire?

Une prise en considération du journalisme d'investigation, contrairement au journalisme d'annonce, laisse transparaître que le journaliste puisse manipuler du 'secret'. Le secret fort nourrissant pour la curiosité, fait vendre. La presse la plus recherchée, la plus vendue est celle qui regorge le plus d'informations occultes possibles. C'est un constat partagé que le journaliste d'investigation vit du secret. Mais la liberté d'expression semble être une arme redoutable aux mains du journaliste contre le concept du secret, tel que nous l'avons abordé. *« La liberté d'expression est un droit pour lequel il faut se battre et non une grâce à implorer ».*[44]

Dans le système juridique français, il y a eu au départ l'article 11 de la Déclaration des droits de l'Homme et du Citoyen du 26 août 1789, qui proclame la *« libre communication des pensées et des opinions*, et autorise tout citoyen à *parler, écrire, imprimer librement, sauf à répondre de l'abus de cette liberté ».*

Il y a eu ensuite la loi du 29 juillet 1881 qui a libéralisé le régime juridique de la publication en supprimant les systèmes de contrôle préventif longtemps en vigueur. Et puis, la loi de 1986 sur la liberté de communication envisage, dans une logique semblable à celle de la loi de 1881, couvre l'ensemble des matières susceptibles de faire l'objet d'une communication audiovisuelle.

[44]Communiqué de presse SG/SM 6978, PI/1128 du 30 avril 1999, la déclaration conjointe faite par le Secrétaire général M. Kofi Annan, le Directeur général de l'Organisation des Nations Unies pour l'éducation, la science et la culture (UNESCO), M. Federico Mayor, et la Haute Commissaire des Nations Unies aux droits de l'homme, Mme Mary Robinson, à l'occasion de la "Journée mondiale de la liberté de la presse".

Enfin, la liberté d'expression est ainsi un droit fondamental qui répond à une conception internationale. L'article 19 de la Déclaration Universelle des Droits de l'Homme du 10 décembre 1945 a consacré la liberté d'expression. Cet article de la Déclaration universelle des droits de l'homme garantit la liberté d'expression dans les termes suivants : *« Tout individu a droit à la liberté d'opinion et d'expression, ce qui implique le droit à ne pas être inquiété pour ses opinions et celui de chercher, de recevoir et de répandre, sans considération de frontières, les informations et les idées par quelque moyen d'expression que ce soit ».* L'article 10 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, proclamée à Rome en 1950 garantit le droit à la liberté d'expression dans des termes analogues à ceux de la Déclaration universelle des droits de l'homme.

En 1966, deux pactes internationaux relatifs aux droits de l'homme ont été adoptés par l'Assemblée générale des Nations Unies et ouverts à la signature des Etats. Ces deux pactes traduisent les droits définis par la Déclaration universelle des droits de l'homme en dispositions précises et contraignantes pour tous les Etats parties. L'article 19 du Pacte international relatif aux droits civils et politiques garantit, de nouveau, la liberté d'expression, en termes similaires à ceux de la Déclaration universelle des droits de l'homme. Le premier protocole à ce Pacte, adopté en même temps, accorde aux individus le droit de se pourvoir directement en appel devant le Comité des droits de l'homme des Nations Unies. Aujourd'hui, plus de quatre-vingt-dix (90) Etats sont parties au Protocole facultatif et le Comité est de plus en plus sollicité. Un dispositif régional de protection des droits de l'Homme, qui garantit particulièrement la liberté d'expression, a été établi en Amérique et un régime de protection a également été institué en Afrique.

Il existe une indéniable corrélation entre la liberté d'expression et la liberté de communication. Le Conseil constitutionnel a essayé de démontrer que la liberté de communication englobe la liberté de presse. Il a précisé que le pluralisme de la presse est un objectif à valeur constitutionnelle[45]. Encore une fois, le communiqué de presse déjà cité résume bien la situation : *« La liberté de la presse est la pierre de touche des droits de l'homme et la garantie de toutes les autres libertés »*[46].

[45]Décision 84-181 DC du 11 octobre 1984, Recueil, p. 78. RJC, p. I-199. Publiée au Journal officiel du 13 octobre 1984, p. 3200.
[46] Ibid., Communiqué de presse SG/SM 6978, PI/1128 du 30 avril 1999

Si la liberté d'expression peut être définie comme la faculté de tout révéler sans inquiétude, ne représente-elle pas représenter une menace au secret ?
Celui qui est libre de s'exprimer n'est logiquement pas astreint au secret au sens de l'article 226-13 du Nouveau Code pénal. Très souvent, l'impact de l'opinion que le journaliste laisse transparaître est si fort que la présomption d'innocence est remplacée par une présomption de culpabilité. Les individus mis en examen ne sont plus 'des suspects,' présumés innocents, mais des 'pré coupables'. La loi sur la présomption d'innocence du 15 juin 2000 [47] s'inscrit également dans la lutte contre la 'justice des médias'. C'est du moins ce qui ressort de la lecture des dispositions relatives à la presse.

Toutefois, il faut noter que la liberté d'expression garantie par la Déclaration universelle des droits de l'homme, la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, et le Pacte international relatif aux droits civils et politiques n'est pas absolue. Chacun de ces instruments définit un certain nombre de limites potentielles à ce droit. C'est dans cette logique que l'article 29 de la Déclaration universelle des droits de l'homme autorise des limitations établies par la loi. Ces limitations ont exclusivement pour but d'assurer la reconnaissance et le respect des droits et libertés d'autrui et afin de satisfaire aux exigences de la morale, de l'ordre public et du bien-être général dans une société démocratique. C'est dans le même esprit que le Pacte autorise des limitations à la liberté d'expression. La Convention européenne contient une liste plus détaillée de restrictions.

Le sens et la portée de ces restrictions ne constituent pas une garantie suffisante au secret professionnel. Il faut trouver un autre sens au secret du journaliste. Dès lors, comment entrevoir le secret professionnel du journaliste ?

Il convient d'analyser la liberté d'expression à contre-pied : être libre de s'exprimer c'est pouvoir se taire quand le besoin s'en ressent. C'est refuser de parler quand on veut sans être inquiété. A cet effet, l'alinéa 2 de l'article 109 du Code de procédure pénale (la loi du 4 janvier 1993) constitue une garantie essentielle du secret du journaliste : *« Tout journaliste, entendu comme*

[47] Loi n° 2000-516 du 15 juin 2000 ; J.O. du 16 juin 2000 p.9038

témoin sur des informations recueillies dans l'exercice de son activité, est libre de ne pas en révéler l'origine ». Ce texte constitue le triomphe de la liberté la presse. En ce sens que le journaliste est le seul citoyen, en France, qui ne soit pas tenu de participer à la manifestation de la vérité. Pourtant, il est sensé être l'individu mieux informé. Le journaliste ne peut être poursuivi d'avoir publié une source qui réclamait la confidentialité et l'anonymat. Une poursuite suppose la preuve d'un contrat entre le journaliste et la victime mais cela n'existe pas.

En conservant l'anonymat de ses sources, le journaliste devient l'instrument par lequel d'autres professionnels astreints au secret échappent à l'article 226-13 du Nouveau Code pénal. C'est ainsi que des détails des comptes bancaires de Roland DUMAS ont pu être publiés dans la presse sans qu'aucun banquier ne soit poursuivi pour violation du secret bancaire.
Aussi, le secret professionnel du journaliste sert de 'bouclier juridique' aux personnes susceptibles de se voir la responsabilité civile ou pénale engagée. Tel était le cas dans l'affaire 'Brad Pitt contre Voici' jugée par TGI de Paris. Les victimes photographiées nus pendant une scène intime, ont voulu que le tribunal oblige le journaliste à indiquer l'identité du photographe. Cela permettrait, par une décision judiciaire, de récupérer les négatifs et d'empêcher toute nouvelle publication. Au non du secret professionnel journaliste, le tribunal n'a pu accéder à la demande des victimes.[48]

« Il existe en effet un devoir, une obligation d'objectivité de la part du journaliste qui peut être sanctionnée par un délit de fausses nouvelles. Mais ces raisons n'ont pas tenu face à la montée en puissance […] de ce que l'on appelle le quatrième pouvoir, c'est-à-dire le pouvoir des médias, lequel doit être assuré par une relative indépendance»[49]. Or le caractère réel et sérieux d'une information tirée du champ su secret professionnel constitue la preuve du recel de violation du secret professionnel. Tel n'est pas l'avis de Maître Christophe BIGOT[50] soutient que *«le recel de*

[48] TGI Paris, 1re ch. ,1re sect., 25 juin 1997, Brad Pitt c. Voici, Legipresse, n° 146.III.140, note Ch. Bigot, *« La protection des sources devant le juge civil »*.
[49] Patrick NICOLEAU, « le secret professionnel du journaliste » in Lexique de droit privé, 1996, ellipses, p.316

[50] Me Bigot est avocat au barreau de Paris spécialisé dans la défense des journalistes. Il représentait également, avec Me Jean-Yves DUPEUX, MM. Albert Du ROY et Guillaume MALAURIE contre le gouvernement français devant la Commission européenne des droits de l'Homme dans l'affaire « Du Roy et Malaurie c. France ». Sur le fondement de l'article 10 de la Convention de sauvegarde des Droits de l'Homme et des libertés fondamentales, les requérants se plaignaient d'une atteinte à leur droit à la liberté d'expression. *« La Cour note que les journalistes qui rédigent des articles sur des procédures pénales en cours doivent ne pas franchir les bornes*

violation du secret professionnel est une négation de la liberté de presse. Si quelqu'un tenu au secret parle, ce qu'il dit devient une information ». A propos de l'arrêt « Fressoz » et autres du 3 avril 1995 de la Chambre criminelle[51], le professeur Emmanuel DERIEUX a exposé une autre vision. *« N'étant pas seulement témoins, mais auteur principal et complices de l'infraction, le directeur de publication et ses différents collaborateurs ne peuvent, dans un tel cas, se retrancher derrière un prétendu droit au secret professionnel »*[52].

L'affaire en question opposait J. CALVET au directeur du *Canard enchaîné*. Les juridictions françaises ont décidé qu'il y avait eu « recel de photocopies…provenant de la violation du secret fiscal ». Cependant, la Cour européenne des droits de l'homme a considéré dans un avis du 13 juin 1998 que les autorités judiciaires (françaises) ont porté atteinte à la liberté d'expression des journalistes. Il ressort de ce qui précède que la question du recel de violation du secret professionnel est l'objet de controverses doctrinales et jurisprudentielles. Elle ne peut être définitivement tranchée que par une loi, ce qui n'est pas encore le cas.

Somme toute, le secret professionnel du journaliste est un secret atypique pour trois raisons :

La première raison est qu'il ne relève pas du régime juridique du secret professionnel tel que prévu par le code pénal. L'article 226-13 du Nouveau Code pénal ne s'applique pas au secret professionnel du journaliste.

La seconde raison est que l'article 109 du Code de procédure pénale affranchit le journaliste de toute obligation de déposer. Il peut refuser de renseigner la justice, sans coup férir. Résultat : le

---

fixées aux fins d'une bonne administration de la justice, et respecter le droit de la personne mise en cause d'être présumée innocente. Cependant, elle observe que l'ingérence litigieuse consiste en une interdiction de publication absolue et générale visant tout type d'information […] En conclusion, la condamnation des journalistes ne représentait pas un moyen raisonnablement proportionné à la poursuite des buts légitimes visés compte tenu de l'intérêt de la société démocratique à assurer et à maintenir la liberté de la presse. Il y a donc eu violation de l'article 10 de la Convention ».

Consultable sur http://www.echr.coe.int/fr/Press/2000/Oct/Du%20Roy%20arret%20fpresse.htm

[51] Cass. crim. 3 avril 1995, JCP 1995.II.22429, note E. DERIEUX, « Publication de documents fiscaux et recel de violation de secret professionnel ».

[52] E. DERIEUX, Droit de la communication, L.G.D.J, 1999, 3e éd., pp.318-334

journaliste peut se retrancher derrière l'article 109 du Code de procédure pénal pour publier des éléments qui relèvent du secret professionnel. Le privilège de confidentialité garanti par le Code de procédure pénal lui permet d'assurer l'impunité des dépositaires réguliers du secret professionnel. Ainsi, le privilège de confidentialité devient-il un privilège d'impunité. D'ailleurs, dans l'arrêt Godwin du 27 mars 1996, la Cour européenne des droit de l'Homme a consacré le secret du journaliste : *« La protection des sources journalistiques est l'une des pierres angulaires de la liberté de presse »*. (Lire également *« L'homme transparent ou la fin de la sphère privée »* de Michel DEROBERT publié dans *Le Temps* des 8 et 9 janvier 2000, cité infra).

Enfin, la troisième raison est que le journaliste est gardien et maître du secret en sa possession. Il en fait ce qu'il veut. Il est libre de divulguer ou non le secret en sa connaissance. Et cette divulgation n'est soumise à aucune autorisation. Cependant, par un arrêt du 19 juin 2001, la Cour de cassation a adressé un sévère avertissement aux journalistes. En effet, la chambre criminelle a confirmé la condamnation de deux journalistes pour *"recel de violation du secret de l'instruction"*dans l'affaire des écoutes de l'Elysée. Les magistrats reprochent à Jean-Marie PONTAUT et Jérome DUPUIS, auteurs du livre *Les Oreilles du président* (Fayard, 1996), d'avoir reproduit des retranscriptions d'écoutes téléphoniques et des procès-verbaux issus du dossier d'instruction du juge Jean-Paul VALAT**.**

Bien que ces reproductions attestent de la véracité de leurs propos, la Cour de cassation a fait primer le respect du secret de l'instruction sur la liberté de l'information. En ce sens, elle a validé un nouvel arsenal juridique contre les journalistes, qui relevaient, jusqu'ici, du seul droit de la presse. De cet arrêt, on peut retenir que le secret de l'instruction prime la liberté d'informer

Les bases de données[53] d'un cabinet médical ou d'avocats, d'une société commerciale ou bancaire (pour ne citer que ceux-là) renferment l'essentiel des dossiers. Le secret professionnel s'étend logiquement aux bases de données et aux courriers du professionnel soumis au secret. Par conséquent, il incombe au professionnel de sécuriser son parc informatique ainsi que tous les flux

[53] Une donnée est une « représentation d'une information sous une forme conventionnée destinée à faciliter son traitement », LAMY Droit de l'informatique et des réseaux éd. LAMY 2002, p. 1927

d'entrées et sorties. L'enjeu de la sécurité est non seulement de garantir l'intégrité des données mais aussi d'assurer leur confidentialité en les mettant à l'abri des surveillants indiscrets.

4-<u>Le secret professionnel à l'épreuve du numérique</u>: une nécessité de protection spécifique et une obligation de sécurité

a- La base de données, des archives numériques dans le domaine du secret professionnel
L'information confidentielle n'est plus archivée uniquement sur le support en papier mais elle est de plus en plus sauvegardée dans des dossiers virtuels sur un support électronique. Le support électronique étant vulnérable, il importe que le professionnel soumis au secret prenne des mesures techniques de nature à protéger son parc informatique et les communications avec ses clients et ses collaborateurs.

La sécurité des données à caractère personnel (les informations relatives au client, au patient…) reste une préoccupation. En effet, l'informatisation des entreprises met en relief des limites de la confidentialité. Cette situation se trouve être une menace au secret professionnel. La protection des bases de données des professionnels astreints au secret s'avère ainsi nécessaire.

Avant de rentrer dans le vif du sujet, qu'est-ce qu'une base de données ?

L'arrêté du 22 décembre 1981 relatif à l'enrichissement du vocabulaire informatique[54] définit la base de données. Selon ce texte, la base de données est *« un ensemble de données organisé en vue de son utilisation par des programmes correspondant à des applications distinctes et de manière à faciliter l'évolution indépendante des données »*. Cette définition a été complétée, tour à tour, par une directive européenne du 11 mars 1996 relative à la protection des bases de données[55] et une loi du 1er juillet 1998[56] qui en est la transposition dans le Code de la propriété

[54] Arr. 22 déc. 1981, JONC 17 janv. 1982, p. 624
[55] Dir. N° 96/9/CE, 11 mars 1996, JOCE 27 mars, n° L 77, p. 20 et s.

intellectuelle (ordre juridique interne). Ainsi, la base de données se trouve être *« un recueil d'œuvres, de données ou d'autres éléments indépendants, disposés de manière systématique ou méthodique et individuellement accessibles par de moyens électroniques ou par tout autre moyen».*

Que faut-il retenir de ces définitions de la base de données ?

En définitive, les bases de données permettent se stocker de l'information structurée par des tables, elles-mêmes contenant un ou plusieurs champs. Par exemple si l'on veut créer un base de clients, on peut créer une table nommée « clients », contenant une structure qui permet de stocker toutes les informations que l'on souhaite pour un client : nom, prénom, adresse, téléphone, e-mail, … Les capacités de stockage et de transfert d'informations permettent de constituer un nombre considérable de réservoirs de données, qu'il s'agisse de chiffres, de textes, de coordonnées personnelles, de références codées ou d'œuvres de l'esprit.

Ainsi, les bases de données du médecin renferment-elles les dossiers médicaux de ses patients. Il s'agit souvent de cet historique qui retrace les antécédents des patients (c'est l'état de santé d'une personne ou même son 'identité sanitaire'); les données médicales signalent les intolérances des patients à certains produits spécifiques (en cas d'urgence et d'hospitalisation etc.), en vue d'un soin plus adéquat.

En somme, ceci constitue une information qui relève de l'intimité de sa vie privée et qui est protégée par le secret médical ; en conséquence, le traitement de cette information nécessite, conformément à l'article 6 de la convention n° 108 du Conseil de l'Europe, le choix de garanties appropriées. Une délibération (n°97-008 du 4 février 1997) portant adoption d'une recommandation sur le traitement des données de santé à caractère personnel rappelle : *«les données de santé à caractère personnel ne peuvent être utilisées que dans l'intérêt direct du patient et, dans les conditions déterminées par la loi, pour les besoins de la santé publique et*

[56] L. n°98-536, 1er juill. 1998, JO 2 juill. 1998, p. 10075 et s.

que, dès lors, leur exploitation à des fins commerciales doit être prescrite. En conséquence, ces données ne peuvent être traitée que dans le respect des droits des personnes et des règles déontologiques en vigueur ».

Il en est de même pour l'avocat dont les bases de données sont le schéma de ses dossiers (ses clients et des informations qui concernent ceux-ci…). Ces données sont souvent réunies aux fins d'une procédure judiciaire. Les bases de données de l'avocat renferment à cet effet le secret de ses dossiers.

b- La protection spécifique des archives numériques

L'arsenal pénal apparaît bien évidemment comme une protection des données qui relèvent du secret professionnel. Mais devant l'anonymat et la dextérité de l'homme, il vaut mieux prendre des mesures de sécurité techniques.

Plusieurs données à caractère personnel sont aussi des 'données sensibles'. La définition de données sensibles est sujette à débat. L'étude du Professeur Spiros SIMITIS[57] met en exergue certaines contradictions.

Néanmoins, les termes de la déclaration commune qui suit fait une synthèse impeccable de données à caractère personnel : *« Dans les secteurs de la gestion du personnel, de la santé, de l'action sociale, de la consommation, des assurances et des banques, les plus voraces en données nominatives, les banques de données prolifèrent. Sous cette pression, les fichiers de données sensibles pour la vie privée se diversifient tant par leur nature (données*

[57] Professeur Spiros SIMITIS du Centre de recherche pour la protection des données, Université Johann Wolfgang Goethe, Francfort, Allemagne, « Les données sensibles revisitées », consultable sous http://www.legal.coe.int

génétiques,...) que par leur utilisation (cartographie sociale ou économique, profils de risques) »[58].

En outre, la Loi Informatique et libertés prévoit une liste de données sensibles dont la collecte et le traitement sont interdits sauf consentement exprès des personnes. Ce sont les données relatives à la race, à l'ethnie, aux opinions politiques religieuses et philosophiques, à l'appartenance syndicale, et aux mœurs.

Les données sensibles tombent naturellement dans le domaine du secret professionnel. Leur caractère 'sensible' impliquant une sécurité toute particulière. Or la confidentialité est un élément de la sécurité des données. C'est pourquoi une exception est donc prévue au profit des professionnels de santé, mais uniquement pour les traitements *« nécessaires aux fins de la médecine préventive, des diagnostics médicaux, de l'administration de soin ou de traitement, ou de la gestion des services de santé et qui sont mis en œuvre par un membre d'une profession de santé, ou par une autre personne à laquelle s'impose, en raison de ses fonctions, l'obligation de secret professionnel prévue par l'article 226-13 du Code pénal»*. L'avocat lié par le secret professionnel bénéficie tout logiquement de cette exception.

Si les données sensibles requièrent une protection particulière, cette protection particulière incombe au professionnel détenteur de ces bases de données. La charge de la confidentialité des données pèse sur eux. Comment organiser la confidentialité des archives numériques ?

L'accès à une base de données se fait en établissant une connexion, c'est-à-dire en précisant l'adresse de la base de données que l'on souhaite visiter, et une identification : nom de l'utilisateur (obligatoire) et mot de passe (pas obligatoire). Un accès non sécurisé permettrait à n'importe quel utilisateur de se connecter et disposer du contenu comme il le souhaite (lecture,

[58] Ligue des Droits de l'Homme, Collectif Informatique, Fichiers et Citoyenneté, Collectif pour les droits des citoyens face à l'informatisation de l'action sociale, Déclaration commune

Consultable sous http://www.delis.sgdg.org

écriture, destruction des données). Un accès semi sécurisé autoriserait par exemple la lecture, mais pas l'écriture ni l'effacement.

Pour l'accès semi sécurisé, deux niveaux de sécurité sont à distinguer :

- *L'accès limité à la lecture*

Dans ce cas l'utilisateur peut lire les informations contenues dans les bases de données mais ne peut ni les modifier, ni les détruire. L'utilisateur ne peut pas disposer des données auxquelles il a accès.

- *L'utilisateur peut modifier ou détruire les données*

'Qui peut le plus, peut le moins' : l'utilisateur qui peut modifier ou détruire des données a nécessairement accès à la lecture.

En somme, la possibilité de modification et la destruction d'une base de données implique l'accès à la lecture, mais l'accès à la lecture n'implique pas forcément possibilité de modification et à de destruction. Tout dépend de la volonté exprimée et l'intention de celui qui crée la base de données. En général, c'est l'administrateur réseau qui est le garant de la sécurité de tout le parc informatique.

c- Une obligation légale de protection : un principe de précaution pour l'environnement numérique ?

Garantir l'intégrité du secret professionnel dans un environnement numérisé revient à garantir une protection efficace des données qui en sont les objets.

L'outil informatique ayant ses faiblesses, les données sensibles font de plus en plus face à la dextérité et à la curiosité dommageables d'utilisateurs 'indélicats'. Cet extrait d'un communiqué d'AFP (Agence Française de Presse) du 12 juin 2000 est saisissant à ce sujet : *« Des fichiers informatiques hautement confidentiels ont mystérieusement disparu du laboratoire américain de recherche sur les armes nucléaires de Los Alamos (sud-ouest), déclenchant une enquête de la sûreté fédérale. Des recherches étendues sont conduites depuis sur les ordinateurs, les coffres-*

forts et les différents aires de stockage des informations du laboratoire dont l'accès est extrêmement restreint en raison des travaux qui y sont conduits sur les armements nucléaires ». De fait, la sécurisation du système informatique d'un professionnel assujetti au secret semble être un impératif. C'est dans cette logique que les données numérisées sont protégées. Les précautions exposées tiennent la confidentialité pour but.

Des logiciels d'authentification et d'autorisation qui limitent l'accès aux données à un code secret sont aussi des moyens techniques permettent de protéger les données sensibles. C'est également ce code secret qui permet d'accéder aux données et aux opérations bancaires à partir d'une carte bancaire.

Cependant, au delà de ces difficultés techniques auxquelles sont confrontés les parcs informatiques, on voit poindre en filigrane une idée-force : le principe de précaution.

Le principe de précaution était au départ un principe du droit de l'environnement. Il a nettement débordé son cadre initial aujourd'hui.

Reconnu tout d'abord par la Déclaration de Bergen (1980), il a été repris par la Convention d'Oslo et de Paris pour la prévention de la pollution marine des 21-22 septembre 1992 et enfin dans la déclaration sur l'environnement et le développement adoptée le 14 juin 1992 lors du sommet de Rio dont l'ambition était de jeter les bases d'un nouvel ordre environnemental universel.

Le principe de précaution, dans cette Déclaration, est formulé dans les termes suivants : *« pour protéger l'environnement, des mesures de précaution doivent être largement appliquées par les Etats selon leurs capacités. En cas de risque de dommages graves, irréversibles, l'absence de certitude scientifique absolue ne doit pas servir de prétexte pour remettre à plus tard l'adoption de mesures effectives visant à prévenir la dégradation de l'environnement ».* Ce principe ne vaut-il pas autant pour l'environnement électronique ?

En fait, il serait question de prendre une mesure ou alors un ensemble de mesures, à titre préventif, pour garantir la sécurité des données et informations sensibles[59].

La cryptographie semble répondre de ce principe de précaution qui est une obligation de moyens et non de résultat, dans la mesure où elle a vocation à garantir la confidentialité des données appelées à circuler. «La question du cryptage des données, en dehors du domaine militaire, pour protéger les informations de toute nature circulant sur la toile s'est posée. Certains y ont vu un outil au service de la liberté de communication tandis que d'autres ont objecté que c'était un outil au service de la criminalité. Le débat semble aujourd'hui dépassé et l'on convient du fait que la cryptographie est, techniquement et juridiquement, un bon moyen d'assurer la confidentialité et la sécurité des échanges sur la Toile »[60].

Qu'est-ce que la cryptographie ? Le dictionnaire Larousse définit la cryptographie comme *« un mode d'écriture secrète au moyen d'abréviation ou de signes convenus »*. Cette définition littéraire ou simpliste laisse échapper toute une réalité technique qui mérite plus d'attention.

D'emblée, il serait intéressant de distinguer la cryptologie de la cryptographie. Ce n'est pas souvent le cas. En résumé, la cryptographie est la science qui a pour but de garder des informations ou des données secrètes. Elle se sert de la cryptanalyse qui est la science qui sert à décoder les informations destinées au secret. La cryptologie n'est en réalité que l'association de la cryptographie et de la cryptanalyse.

Selon Alain BENSOUSSAN, on entend par prestations de cryptologie *« toutes prestations visant à transformer à l'aide de conventions secrètes des informations ou signaux clairs en en informations ou signaux inintelligibles pour des tiers, ou à réaliser l'opération inverse, grâce*

[59] « L'information sensible est une information dont l'importance est telle qu'il faut en assurer la confidentialité et l'intégrité », Lamy Droit de l'informatique et des réseaux, éd. Lamy 2002, p. 1933

[60] ROUJOU DE BOUBEE Isabelle, *Cryptographie : ses nécessités, ses dérives* in Les libertés individuelles à l'épreuve des NTIC , études réunies sous la direction de Marie-Christine PIATTI, éd. Presse Universitaire de Lyon (PUL), 2001, p.125

à des moyens ou des logiciels conçus à cet effet »[61]. (Voir loi n°90-1170 du 29 décembre 1990 art.28 I)

L'hypothèse du risque n'étant jamais totalement exclue dans le système informatique, il est compréhensible que la cryptographie soit la cause des thèses les plus optimistes en matières d'échange de données par Internet. Ainsi, sous la plume du professeur Jean DEVEZE peut-on lire : *« La technique informatique fournit les parades aux faiblesses qu'elle engendre...La fidélité du contenu de l'information transmise et sa confidentialité peuvent être garanties de façon quasiment absolue par les techniques de cryptage »*[62]. J. Stern[63] assurait également par ces mots : *« Avec Internet, la cryptologie est passée de la science du secret à celle de la confiance ».*

La dernière affirmation serait à l'abri de toute critique si elle ne semble pas écarter le secret des buts de la cryptologie. Le secret, qu'il relève du domaine militaire ou civil, repose sur la confiance. Vus d'une certaine manière, les deux vont toujours de paire. D'ailleurs, dans une étude consacrée à la sécurité des réseaux, Philippe DEJEAN a précisé que *« la sécurité d'une information se confond avec, sa confidentialité, son intégrité et sa disponibilité »*[64]. L'assertion de J. Stern cache une autre problématique que nous rappelons ici pour mémoire : la valeur probatoire de l'écrit et de la signature électroniques[65].

La messagerie électronique du professionnel dépasse les 70% des activités sur Internet. Or le professionnel perd toute maîtrise des données confidentielles dont il a la responsabilité

---

[61] Alain BENSOUSSAN, Informatique et télécoms, éd. Francis Lefebvre, 1997, p.695

[62] André LUCAS, Jean DEVEZE, Jean FRAYSSINET, Droit de l'informatique et de l'Internet, éd. Thémis, nov.2001

[63] J. STERN est Directeur du laboratoire informatique de l'Ecole Normale Supérieure

[64] Philippe DEJEAN, Puissance publique et sécurité des réseaux in Les nouvelles pratiques liées aux technologies de la communication, actes des 10 journées organisées par le Magistère en Droit de la communicatique, éd. PUF, 1999, pp.123-130

[65] Voir la directive européenne n°1999/93/CE du 13 décembre 1999 sur un cadre juridique pour les signatures électroniques, Gaz. Pal., 29, 31 octobre 2000 ; la loi du 13 mars 2000, article 1316-4, Code civil 2001 Dalloz et son décret d'application du 30 avril 2001, J.O. n° 77 du 31mars 2001p. 5070, Legifrance, l'essentiel du Droit français.

pendant le transfert. Il convient, dès lors, de protéger les EDI (échange de données informatisées) relevant du secret professionnel.

La cryptographie se trouve être garante de la confidentialité et de la sécurité des EDI. Des logiciels de cryptage sont de plus en plus utilisés et de plus en plus variés. A titre illustratif, les logiciels à clé secrète cèdent la place aux logiciels à clé publique dans lesquels une clé servant à chiffrer les données est rendue publique. En revanche, la clé qui sert à déchiffrer les données est secrète et n'est transmise qu'au destinataire des données chiffrées.

La banque est aujourd'hui, avec le développement de l'*e-banking ou telebanking,* un terrain fertile de l'informatisation. Une banque remet à son client un cd-rom ou une disquette la clé publique étant déjà envoyée à tous les clients via réseau, sous une certaine confidentialité, lequel va lequel va installer sur son ordinateur un 'e-wallet' appelé portefeuille électronique. On l'ouvre à chaque fois que le besoin de transaction électronique se présente.

On y gagne du temps. La banque peut s'assurer de l'origine du message en le décryptant avec sa clé publique. Le client pour sa part peut crypter ses messages au moyen de sa clé secrète. Non seulement le cryptage garantit dans un tel cas la confidentialité des données mais aussi elle vaut signature. Le client d'une banque peut ainsi envoyer à son banquier un ordre de virement, de mise en vente de ses titres en bourse grâce au cryptage.

Les avocats dans le partage du secret professionnel peuvent protéger leurs messages par le cryptage. Les avocats d'affaires utilisent la cryptographie pour communiquer avec leurs clients qui sont souvent des firmes soucieuses de protéger leur image de marque.

Quel est le coût de la sécurité pour les entreprises ou les personnes qui l'utilisent ?

La question de la sécurité est mieux cernée a contrario. C'est généralement en l'absence de la sécurité que l'on apprécie mieux la sécurité. Dès lors, quel est le coût de la non sécurité pour le professionnel ?

A quoi servirait cet avocat, ce banquier, ce notaire ou alors ce prestataire technique à qui l'on ne peut pas faire confiance en fonction du caractère aléatoire de son système informatique (risque de pertes des données (preuves et moyens de défense), la facilité des intrusions menaçant la confidentialité etc.) ? La conséquence logique de cet état de fait est la perte des clients. Il y a aussi toutes les difficultés que l'imagination met à notre disposition.

Dorénavant, il est possible à l'expéditeur de fixer la durée de vie de la clé qu'il envoie avec le message chiffré. Au terme du délai prévu, qui varie entre quelques secondes et plusieurs années, la clé s'autodétruit et le message deviennent irrémédiablement illisibles[66]. Ce système se prête parfaitement à la communication rapide de données entre professionnels, entre professionnels et clients ou entre particuliers en raison de son caractère confidentiel.

Le défaut de sécurité est une menace à la vie privée. On peut se demander quel est le rapport. Or, même si elle n'est pas physique ou directe, en touchant aux données personnelles qui relèvent de la vie privée, on touche à l'homme lui-même. Ainsi, de la sécurité de la personne virtuelle surgit la sécurité la personne réelle.

Le poids de la sécurité des systèmes d'information dans le budget des entreprises et des cabinets est très variable, mais la DCSSI (Direction Centrale de la Sécurité des Systèmes d'Information) observe une prévision d'entre 2 et 3 % en général.

C'est en effet la DCSSI instituée par décret le 31 juillet 2001[67] assure la fonction d'autorité nationale de régulation pour la SSI[68]. Elle délivre les agréments, cautions ou certificats pour les systèmes d'information de l'État, les procédés et les produits cryptologiques employés par l'administration et les services publics, et en contrôlant les centres d'évaluation de la sécurité des technologies de l'information (CESTI). Elle a d'autre missions : elle contribue à la

[66] Voir http://www.liberation.fr/index.php, *«Trois blindages annoncés »,* le 18 octobre 1999

[67] Décret n°2001-693 du 31 juillet 2001 créant au secrétariat général de la défense nationale une direction centrale de la sécurité des systèmes d'information Elle est placée sous l'autorité du Secrétaire général de la défense nationale.

[68] Sécurité des systèmes d'information

définition interministérielle et à l'expression de la politique gouvernementale en matière de sécurité des systèmes d'information ; elle évalue les menaces pesant sur les systèmes d'information, donner l'alerte, développer les capacités à les contrer et à les prévenir (CERTA) ; elle assiste les services publics en matière de SSI ; elle développe l'expertise scientifique et technique dans le domaine de la SSI, au bénéfice de l'administration et des services publics ; elle forme et sensibiliser à la SSI (Centre de formation à la sécurité des systèmes d'information - CFSSI). Le Service Central de Sécurité des Systèmes d'Information (SCSSI) a pour mission de garantir la sécurité des réseaux.

En outre, si nous admettons que l'obligation qui pèse sur le professionnel est une obligation de moyens, il ne devra répondre de l'effusion de l'information confidentielle à sa charge que s'il n'avait pas pris les mesures nécessaires à sa protection. Ce serait le cas du professionnel qui après avoir travaillé sur un ordinaire, ne ferme pas sa session qu'il ouvre au moyen d'un code secret. Ce peut être également le cas du professionnel négligent qui envoie des données sensibles sans les avoir cryptées au préalable.

Conscient de la responsabilité du professionnel soumis au secret et de la fragilité du système informatique, Lionel BOCHURBERG qui est avocat avertit en ces termes : *« le cabinet d'avocat doit assurer une confidentialité à ses échanges, étant tenu au secret professionnel»*[69]. L'avertissement de cet avocat est respectueux de l'article 29 de la loi L. n°78-17 du 6 janvier 1978 *relative à l'informatique, aux fichiers et aux libertés*[70]. En vertu de cet article, « toute personne ordonnant ou effectuant un traitement d'informations nominatives s'engage de ce fait, vis-à-vis des personnes concernées, à prendre toutes les précautions utiles afin de préserver la sécurité des informations et notamment d'empêcher qu'elle ne soient déformées, endommagées ou communiquées à des tiers non autorisées ». En définitive, c'est d'abord sur cet article que se fonde l'obligation de sécurité.

[69]Lionel BOCHURBERG, *Internet et commerce électronique*, 1re éd. DELMAS 1999, pp.135-151

[70] La loi du 6 janvier 1978 a été modifiée par les lois n° 92-1336 du 16 décembre 1992 relative à l'entrée en vigueur du nouveau Code pénal, n° 94-548 du 1er juillet 1994relative aux données nominatives ayant pour fin la recherche dans le domaine de la santé et la loi n° 2000-321 du 12 avril 2000 relative aux droits des citoyens dans leurs relations avec l'administration.

Quelle est la nature du terme « s'engage » contenu dans l'article 29 de la loi de 1978 et quel sens faut-il lui accorder ? Au fait, le législateur n'entendait en aucune façon créer par ce mot un engagement contractuel. Il s'agit évidemment d'une obligation légale. La méconnaissance de cet article constitue un délit. Un arrêt de la Chambre criminelle du 19 décembre 1995[71] l'a d'ailleurs confirmé. En l'espèce, les mesures étaient prises mais se sont avérées insuffisantes pour éviter les risques d'homonymie et de fausses informations.

La Directive communautaire 95/46/CE du 24 octobre 1995 est *« relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel »*. Elle a pour objectif d'établir *« une protection équivalente de haut niveau dans tous les Etats membres de la Communauté afin d'éliminer les obstacles aux échanges des données nécessaires au fonctionnement du marché intérieur ».*

Le contenu de cette directive est proche de celui de la Loi de 1978. Mais en tant que directive, seul un acte de transposition pourrait en garantir l'efficacité en droit interne. Toutefois il faut reconnaître que le régime d'effet direct créé par la Cour de justice des Communautés européennes permet aux directives communautaires non transposées de s'intégrer directement dans l'ordonnancement juridique des Etats[72].

Cela étant, le Gouvernement Jospin a rendu public, le 24 juillet 2001, un projet de loi modifiant la loi Informatique et Libertés, afin de transposer la directive communautaire du 24 octobre 1995 relative à la protection des données à caractère personnel. Ce projet de loi a été transmis au Parlement et fera vraisemblablement l'objet d'un vote et d'une promulgation au cours de cette année (2002). Il englobe plusieurs dispositions susceptibles de réformer le cadre légal et réglementaire actuel du traitement des données nominatives.

[71] Cass, crim., 19 décembre 1995, JCP, éd. G1996, IV, n° 702, D. 1996

[72] Cependant les juges nationaux « rechignent » souvent à appliquer aux directives communautaires un effet direct et notamment le Conseil d'Etat français qui réfute tout effet direct des directives: CE, 22/12/1978, Cohn-Bendit, Rec., p.524

L'innovation de la transposition de la directive communautaire de 1995 et le projet de loi dans son article 8 est l'institution d'un régime particulier relatif au traitement des données de santé, celles-ci seront dorénavant considérées comme des données sensibles interdites, sauf consentement des personnes.

Le Code pénal sanctionne également la non protection des données personnelles. L'article 226-17 du Code pénal réprime le fait de procéder au traitement de données nominatives sans prendre les précautions nécessaires pour en préserver la sécurité et la confidentialité[73].

Toutefois, il faut remarquer que si la législation prévoit une obligation de sécurité (une obligation de « précaution ») qui est manifeste, elle n'impose pas de moyens précis permettant d'y aboutir. Par conséquent, la preuve de cette obligation de sécurité (obligation de moyens) pourrait se faire par tous moyens. Nous pouvons prendre également l'exemple du réseau du notariat qui est une plate-forme Intranet (réseau fermé) à laquelle les notaires accèdent avec leur carte à puce Réal et un code d'accès confidentiel. C'est grâce à une collaboration avec la Société *Communication et Signaux* (CS) qui a permis de mettre ce système en place. La CS est engagée dans le programme européen OSCAR d'échanges sécurisés. La technologie mise en œuvre s'appuie sur les solutions de sécurité CS-Webp@ss, CS-CIPHER et CS-SmartPKI développées par le groupe CS. Ce système a permis au Conseil Supérieur du Notariat de créer les conditions les conditions de reconnaissance des actes notariés électroniques. Des actes notariés circulent ainsi entre notaires assujettis au même secret professionnel. Enfin, ce système relie des notaires de différentes nationalités européennes grâce à l'avènement de l'acte authentique électronique.

En conclusion, il appartient au juge du fond d'en juger de façon souveraine, en fonction des circonstances particulières et de l'attitude du professionnel en cause, si ce dernier a protégé les données confidentielles.

[73] Article 226-17 du Nouvel Code pénal : «Le fait de procéder ou faire ou de faire procéder à des traitements automatisés d'informations nominatives sans prendre toutes les précautions utiles pour préserver la sécurité de ces informations et notamment empêcher qu'elles ne soient déformées, endommagées ou communiquées à des tiers non autorisés est puni de cinq ans d'emprisonnement et de 2 000000 franc d'amende » ; (Voir également l'article 226-16 NCP).

Une autre question mérite, au cours de cette réflexion d'ensemble que l'on s'y arrête pour en saisir le sens et la portée : la cybersurveillance. Sujet d'actualité, il l'est, sans doute. Mais sujet ennuyeux, il l'est également. Il est judicieux qu'un débat s'ouvre à son propos. Dès lors, qu'est-ce que la cybersurveillance et en quoi se justifie-t-elle (missions, bases légales…) ?

Chapitre II : La cybersurveillance comme mesure administrative ou judiciaire

Ce deuxième chapitre sera consacré aux notions de cybersurveillance et de police administrative (1), à la cybersurveillance dans la lutte contre la cybercriminalité (2), à la vidéosurveillance (on se demande si elle constitue un dispositif de sécurité ou une garantie contre l'arbitraire) (3) et enfin aux écoutes téléphoniques qui s'apparente tantôt à l'espionnage, tantôt à l'enquête judiciaire (4).

1- <u>Les notions de cybersurveillance et de police administrative</u>

a- Qu'est-ce que la cybersurveillance ?

L'expression anglaise *to keep watch* signifie surveiller au sens de contrôler et vérifier. On peut dire que surveiller un sujet c'est le garder sous son contrôle, en le regardant. La surveillance vue sous cet angle ne requiert pas l'adhésion de la personne qui y est soumise. C'est un acte d'autorité.

Comment définir la cybersurveillance ?

L'embarras surgit dès lors qu'on se propose de définir la cybersurveillance. Il n'y a pas de définition unique de la cybersurveillance. Mais à partir des éléments épars de différents points de vue, une définition est envisageable.

D'entrée, le préfixe *cyber* tiré de la cybernétique s'emploie dans des composés relatifs aux réseaux numériques de communication. Or le mot 'cybersurveillance' est composé du préfixe *ciber* et du radical *surveillance*. Donc nous pouvons admettre que la cybersurveillance est la surveillance des réseaux de télécommunication. Que faut-il entendre par 'réseaux de communication' ?

Selon l'article 2 de la loi du 29 décembre 1990 sur la réglementation des télécommunications, les réseaux de télécommunication sont les installations qui assurent « la transmission, la transmission et l'acheminement de signaux de télécommunications ainsi que l'échange des informations de commande et de gestion qui y est associé, entre les points de terminaison de ce réseau ». Nous pouvons en déduire que le réseau de transmission de données est l'ensemble des tuyaux de transmission de données et moyens techniques qui permettent l'interconnexion des terminaux de données. Autrement dit, la cybersurveillance est l'ensemble des voies et moyens aboutissant à l'accès, au contrôle des données ou signaux transmis par voie électronique ainsi que le contrôle des moyens techniques permettant ces transmissions. Par l'installation d'un logiciel de surveillance permet d'enregistrer tous les événements survenus sur un ordinateur : enregistrement des frappes clavier, dates et heures d'ouverture et de fermeture de sessions Windows, les logiciels utilisés, les documents ouverts, créés ou supprimés…bref, toutes les actions d'un utilisateur avec des captures d'écran.

Le caractère oral ou virtuel des signaux ciblés par la cybersurveillance est indifférent. De ce fait, les écoutes téléphoniques font partie intégrante de la cybersurveillance. En résumé, la cybersurveillance permet contrôler et de suivre à la trace les internautes au travers des données échangées en réseau et en ligne. Elle permet plus globalement de contrôler les usagers des moyens de communication en ligne : Web (Internet et Intranet), téléphone, téléphone portable, fax, télégramme etc.

La définition de la cybersurveillance implique également la vidéosurveillance, le Web Cam dans les lieux publics ou dans le cadre plus restreint des entreprises. Celle-ci permet de filmer dans un environnement déterminé les individus et leurs comportements. Elle permet d'établir la preuve difficilement réfutable d'une infraction ou d'un incident, même technique.

On peut pousser l'analyse plus loin et se demander si la boîte noire d'un avion ne rentre pas tout naturellement dans les éléments de la cybersurveillance. En effet, la boîte noire permet d'enregistrer les communications à bord de l'avion. On peut la comparer à un 'cookie'. Le 'cookie' étant ce petit fichier envoyé par un gestionnaire de site sur le disque dur de l'utilisateur permettant d'identifier celui-ci lors de sa connexion au site et de mémoriser celle-ci. La boîte noire enregistre également les communications établies entre un avion et des contrôleurs aériens.
Dans cette hypothèse d'école, nous pouvons faire deux remarques :-la première est qu'il y a communication en réseau, même si c'est un réseau fermé. Deuxième remarque : ces communications sont conservées en vue d'asseoir d'éventuelles explications d'ordre divers (cela nous est indifférent), de faire la preuve de certains faits. Les paroles des terroristes du 11 septembres enregistrées par les boîtes noires des deux appareils d'American Air Line sont des éléments d'une précieuse valeur probatoire. Même si les commanditaires ont revendiqué les attentats, en cas de procès elles seraient d'une grande utilité. Les attentats ont mis fin à l'existence des avions et de ceux qui étaient à bord de ce dernier. Tout ce qui reste -et c'est le seul témoin crédible- le seul surveillant survivant, semble être la boîte noire. Il est vrai que la situation d'une boîte noire n'est pas celle d'une caméra qui surveille dans un lieu public ou dans une entreprise mais leurs finalités ne sont-elles pas analogues ?
La présence de caméra est dissuasive presque comme le regard vigilant d'agents de police. N'est-ce pas comme cela que l'autorité municipale a expliqué la mise sous vidéosurveillance de la ville de Levallois ? Cependant, une nuance doit être faite car la boîte noire d'un avion n'a pas vocation à dissuader et à traquer. Or c'est en cela que l'on redoute la télésurveillance. En outre, la boîte noire enregistre en vue d'une expertise : sa mission semble purement technique ou à tout le moins scientifique, tandis que les données enregistrées sur le Web et le Web Cam tout comme les sons enregistrés lors d'une écoute téléphonique constituent des preuves contre des personnes surveillées. Enfin, tout 'administrateur réseau robotisé' de bord, la boîte noire, dans son autonomie, peut aussi servir la cause d'une enquête. Mais on ne peut pas dire qu'il s'agit véritablement d'un instrument de surveillance. L'enjeu d'une boîte noire semble bien différent de la cybersurveillance, du moins dans le système aéronautique. Néanmoins, le fait d'équiper les véhicules de boîte noire pour déterminer le comportement des conducteurs au volant (vitesse etc.), peut justifier une objection. Surtout si l'on sait que les gouvernements allemand et français

envisagent de la placer dans les véhicules des délinquants du Code de la route : c'est la liberté sous surveillance électronique. Faut-il l'appeler cybersurveillance ou pas ?

Par ailleurs, un chirurgien anglais, Ara DARZI, du *London Imperial College* vient d'inventer un autre usage à la boîte noire. La boîte noire surveillera désormais les salles d'opération et enregistrera les faits et gestes des chirurgiens. Des capteurs électromagnétiques et supersoniques installés sur les mains du praticien enregistreront tous les détails de l'intervention, des instruments utilisés aux conversations, en passant par les allées et venues du personnel. Selon son concepteur, « la salle d'opération est comme la cabine de pilotage d'un hôpital »[74]. Faut-il parler de cybersurveillance ou pas ? Pour l'heure, avant l'obtention d'un brevet, le concepteur doit faire face aux critiques qui assimilent cette boîte noire à un mouchard susceptible d'accentuer la pression déjà grande en salle d'opération. Salle d'opération, zone de secret. Secret professionnel.

Toute opération qui transite sur un ordinateur laisse des traces. La référence la plus simple est le fichier « log ». Celui-ci permettant de remonter jusqu'à l'utilisateur constitue un élément de traçabilité et la preuve des opérations effectuées. La recherche de traces opérées sur un ordinateur relève de la cybersurveillance.

La cybersurveillance semble être, par essence, un mode de preuve. Or la preuve est au service de la police judiciaire (ou encore d'une action civile éventuelle) et non pas de la police administrative. La police administrative est, tout au plus, dissuasive. Elle est une fin en soi : le maintien de l'ordre public, tandis que la police judiciaire n'est qu'un moyen : elle cherche à livrer un suspect à la justice et à établir la preuve de sa culpabilité. Il est délicat d'établir la limite entre les deux missions de police.

b- Qu'est-ce que la police administrative ?

Très souvent, le maintien de l'ordre public explique la police administrative. Le maintien de l'ordre public réside dans l'édiction de normes accompagnées d'actes matériel. La police peut être

[74]Aurélie DELEGLISE, La boîte noire double-emploi, 29/08/2001,
consultable sous http://www.cybersciences.com/cyber/3.0/N2464.asp

entendue comme l'ensemble des mesures qui régentent les rapports en société en vue d'y garantir le maintien de l'ordre public.

D'emblée, il importe de définir l' 'ordre public'. L'ordre public est un concept au contenu évolutif et variable suivant les époques et les systèmes juridiques. Toutefois, la finalité de l'ordre public semble immuable : il permet le bon fonctionnement des institutions, facilite la vie sociale des citoyens et garantie la sécurité des citoyens. Une trilogie bien connue fait de l'ordre public un ensemble de sécurité, salubrité et tranquillité publiques. Cette trilogie bénéficie de la compagnie bonnes mœurs comme l'a prévue l'article 6 du Code civil[75]. Cependant, l'importance de la sécurité publique dans le concept de l'ordre public comme prétexte des mutations législatives et juridiques actuelles indiquent notre choix. Choix qui nous conduira à nous attarder davantage sur la sécurité publique dans les lignes suivantes, après une définition d'ensemble.

Le maintien l'ordre public est l'élément essentiel de la police administrative générale. Assurer l'ordre public, c'est prendre des mesures de nature à prévenir et éviter de désordre, si l'on considère l'ordre comme la situation 'normale'. La police administrative a pour fin d'allier le respect concomitant des activités et relations privées avec le respect de l'intérêt général. Elle a pour but de maintenir l'ordre public.

La validité de la police administrative peut être vue sous l'angle de la validité matérielle. Il ne s'agit pas d'un ordre public prévu par des normes mais un ordre public instauré et vécu qui constitue la police administrative si l'on se réfère à la théorie réaliste à la ROSS.
On parlera dès lors de police administrative lorsque le maintien de l'ordre public n'est pas un concours de circonstances mais un climat spécial (la trilogie traditionnelle) créé et maintenu par l'autorité publique.

[75] Article 6 du Code civil : « on ne peut déroger par conventions particulières, aux lois qui intéressent l'ordre public et bonnes mœurs ».

On ne saurait ignorer que seules des circonstances locales justifient l'ordre public.[76] Qu'est- ce donc la trilogie traditionnelle ? Et pourquoi 'traditionnelle', y a-t-il quelque chose de nouveau, ou peut-on étendre cette trilogie ?
Traditionnellement les composantes de l'ordre public correspondent à la tranquillité, la sécurité et la salubrité publiques.

La sécurité publique est l'absence d'atteinte aux personnes et aux biens. Elle est également la prévention contre les calamités ou catastrophes naturelles : les crues et incendies… et contre les actes de malveillance : la violence urbaine, le viol, …aujourd'hui un fléau social vieux comme le monde fait recettes (l'insécurité).

Quant à la salubrité publique, elle concerne la santé et l'hygiène des personnes et tend à empêcher l'extension d'épidémies touchant une société donnée (les campagnes de lutte contre le sida, la campagne de vaccination contre l'hépatite B en France.
La salubrité publique peut être définie mieux qu'une absence de maladies ou de difficultés sanitaires pour représenter l'idée d'un bien-être général. Cette définition peut paraître bien éloignée des réalités mais si l'on estime que la notion de police administrative qui est un idéal abrite une certaine zone d'utopie, elle peut être intéressante. Enfin, assurer la tranquillité publique, c'est vaincre au maximum les gênes que peuvent subir les individus dans leur vie quotidienne (les nuisances sonores etc.).

En 1995, le Conseil d'Etat a affirmé que même en dehors de circonstances locales particulières, une activité pouvait être interdite si celle-ci portait atteinte à la dignité humaine (C.E. Ass. 27 octobre 1995, Commune de Morsang-sur-Orge et CE Ass, 27 octobre 1995, Ville d'Aix-en-Provence à propos des spectacles de "lancer de nains"). Une partie de la doctrine estime que cet arrêt du Conseil d'Etat est une extension de la trilogie traditionnelle. Car désormais un élément nouveau a été ajouté à la liste : la dignité de la personne humaine. Il était, par conséquent, hors de question que les symboles du nazisme puissent faire l'objet de publicité sur Internet. Une lecture

[76] C.E. sect. 18 décembre 1959, Société les Films Lutétia

sommaire de la jurisprudence dite « Yahoo »[77] suffit à donner l'impression que la cybersurveillance est une nécessité sociale, une mission de l'administration.

c- La dignité humaine comme élément de l'ordre public

La lutte contre la circulation des contenus affectant la dignité humaine sur Internet s'avère nécessaire. A priori les échanges d'images à caractère pornographique sur le Web ne semblent pas poser grand problème à l'ordre public. Car, en réalité, combien sont-ils à refermer les fenêtres donnant accès à ces images ?

Avec l'avancée de la pornographie s'est posée la question de la protection des enfants (« les mineurs »). La jurisprudence est catégorique à cet égard. En effet, respecter la dignité des enfants c'est aussi éviter de les soumettre à des scènes qui heurtent leur sensibilité. La pornographie n'est pas illicite en soi, et la loi n'interdit pas la pornographie aux adultes. Il n'en est pas de même lorsque les enfants y sont impliqués (comme acteurs ou spectateurs).

La pornographie dépassant volontiers le désir sexuel, les scènes qu'elle offre ne sont pas souvent des démonstrations d'affection. A cela s'ajoute la pédopornographie sur Internet. A cet égard, il y a lieu de noter non seulement la cruauté de l'exploitation des enfants à la cause de la prostitution et de la pornographie, mais aussi leur exposition à ces images sur Internet. Comment protéger la dignité humaine sans protéger les mineurs ?

Il importe que des mesures, de toute nature, puissent protéger les mineurs. Il convient de rappeler les apports du Conseil d'Etat et notamment une étude de la Section des du rapport et des études intitulée *Internet et les réseaux numériques* adoptée par l'Assemblée générale du Conseil d'Etat le 2 juillet 1998. (Lire également le rapport d'information de M. Alain VIDALIES du 12 décembre 2001)[78]. Pour mieux renforcer la lutte contre la pédopornographie via Internet, le Code pénal fait montre d'une sévérité dissuasive. La loi du 4 mars 2002 relative à l'autorité parentale,

[77] Référé, TGI Paris, aff. UEJF et Licra c/Yahoo ! Inc. et Yahoo France, 22/05/2000
[78]Rapport n°3459, consultable sous http ://www.assemblee-nat.fr/rap-info/i3459.asp

les articles 227-23 et 227-24 du Code pénal sont des marques de cette politique pénale. (Voir la partie consacrée à la cybercriminalité…infra).
Mais la réalité montre que les mineurs ont accès à ces interdits via la télévision par satellite, l'usage de l'Internet etc. Comment rendre efficace toutes ces mesures en dehors de la surveillance, mais comment surveiller les individus dans leurs relations privées sans porter atteinte au droit au respect de la vie privée ? Doit-on filtrer les données échangées en réseau et les sites Internet? Si l'on accepte le filtrage, alors la cybersurveillance devient techniquement nécessaire. Et si la cybersurveillance devient nécessaire, elle donne accès à tous les secrets de la vie courante, y compris le secret professionnel.

La question s'est posée de savoir si l'ordre moral entrait dans la définition de l'ordre public. La jurisprudence considère que l'ordre moral ne doit être pris en compte dans l'ordre public que si le désordre moral peut aboutir à un désordre matériel[79].
Outre la question de l'ordre moral, juge administratif a refusé d'admettre la référence à l'esthétique dans la définition de l'ordre public. Par conséquent, un maire ne peut, pour des motifs d'ordre esthétique, imposer des normes particulières aux monuments et plantations d'un cimetière (C.E. 1983, Commune de Bures-sur-Yvette).

La police, c'est aussi l'ensemble des personnes ayant pour mission de faire appliquer ces mesures. La police administrative est exercée par les autorités publiques et elle a un caractère inaliénable. Cela va sans dire que l'exercice de la police administrative ne peut faire l'objet d'une concession au profit d'une personne privée[80].

L'efficacité de l'action publique s'inscrit aujourd'hui dans une approche large du contrôle des activités par l'administration. L'ancien administrateur colonial du Mali Hamadou HAMPATE-BÂ[81] disait qu'«un chef, un administrateur, qui ne sait pas ce qui se passe sur son territoire n'en est pas un». Il faut, à l'évidence, relativiser cette affirmation dans le contexte actuel. Mais la nécessité de la présence et surtout du contrôle de l'administration semble bien constante à travers

[79] C.E. sect. 18 décembre 1959, Société les Films Lutétia**,** CE 19 avril 1963, Ville d'Avranches
[80] C.E. 1904, Dame Breysse
[81] Ahmadou HAMPATE-BÂ était surtout connu comme écrivain de l'Afrique francophone. *L'étrange destin de Wangrin* reste un chef-d'œuvre qui l'a rendu célèbre.

le temps et les régimes politiques. L'ordre juridique s'y adapte en général. L'étude de la Loi Sécurité Quotidienne arborera plus loin la cybersurveillance comme un instrument de protection de l'ordre public en général et de lutte contre le terrorisme en particulier. Cela veut dire que l'action publique s'adapte à l'environnement électronique de sorte qu'il n'échappe pas à son contrôle.

Quel rapport y a-t-il entre la police administrative et la cybersurveillance ? Rien d'extraordinaire, à voir de près. C'est juste une symbiose et une adaptation des moyens de contrôle de l'administration : la cybersurveillance peut être un instrument de la police administrative et la police administrative peut être un fondement légal de la cybersurveillance.

Les analyses suivantes nous permettront de mieux cerner la cybersurveillance au travers de ces différents modes et finalités.

2- La cybersurveillance dans la lutte contre la cybercriminalité

a- L'extranéité de la cybercriminalité et la nécessité d'une harmonisation juridique internationale

L'adoption du premier traité international de lutte contre la contre la criminalité dans le cyberespace par les Délégués des Ministres du Conseil de l'Europe le 19 septembre 2001[82] a marqué un tournant décisif dans la lutte contre la cybercriminalité. Cette convention concerne les infractions pénales commises via les réseaux de communication en général et l'Internet en particulier. Elle prévoit pour être efficace une série de mesures que nous pouvons nommer à juste titre la 'cyberprocédure' pénale. Il s'agit de la perquisition de réseaux informatiques et l'interception des e-mails. Ces nouvelles procédures faciliteront la conduite des enquêtes judiciaires, et fixe des règles de coopération internationale en matière de crimes et délits.

[82] Convention sur la cybercriminalité, consultable sous http://press.coe.int/cp/2001/646f(2001).htm
Cette convention a été ouverte à la signature le 23 novembre 2001, lors d'une conférence internationale organisée à Budapest les 22 et 23 novembre 2001. Trente Etats ont signé la Convention. Quatre Etats des 30 Etats signataires n'étaient pas membres du Conseil de l'Europe mais ont participé à l'élaboration du traité.

Chaque Etat signataire va créer un « point de contact » joignable 24/24 h, 7 jours sur 7 pour recueillir les preuves sous forme électronique)… Bref, cette convention est la reconnaissance légale au plan international de la cybercriminalité et la cybersurveillance comme moyens de lutte contre la cybercriminalité.

En effet, l'Internet, comme la plupart des réseaux de télécommunication, met en relief les limites des législations et actions publiques nationales. La cybercriminalité ne connaît pas de frontière. Ce sont seulement une harmonisation législative et une réelle coopération internationale qui seraient la garantie d'efficacité des mesures répressives. La recevabilité d'un exequatur est d'ailleurs à ce prix. L'affaire «Yahoo» restera un exemple éloquent de la contradiction des législations ayant entraîné l'échec de la coopération internationale pourtant nécessaire. Le juge Gomez s'est heurté à une interprétation laxiste de la liberté d'expression de son homologue américain à propos de l'exposition d'objets nazis et contenus révisionnistes : « Vérité en deçà des Pyrénées, erreur au-delà »[83]. Nonobstant cette vision de Pascal qui traduit très bien la contradiction ou alors la différence des lois au-delà des frontières, la porosité des frontières ne saurait être un obstacle à l'action publique.

L'harmonisation européenne de la lutte contre la cybercriminalité s'inscrit dans cette optique. La Commission européenne a publié le 23 avril 2002 une proposition de « décision cadre » relative aux attaques des systèmes d'information. Cet acte vise à harmoniser les droits pénaux et les moyens d'action des différents Etats membres dans la lutte contre la cybercriminalité. Elle énumère un certain nombre d'infractions propres à l'environnement numérique : l'accès illicite à des systèmes d'information, la fraude informatique, atteinte à l'intégrité des données, injection de virus, pédopornographie, piratage (distribution à grande échelle de copies illégales d'œuvres protégées) etc.

A ce niveau, un constat paraît nécessaire : l'informatique ou les réseaux peuvent être le moyen de l'infraction ou l'objet de l'infraction.

[83] Blaise Pascal, Les Pensées

b- Les contenus illicites et illégaux

L'échange ou le commerce d'objets illicites sur Internet constitue une infraction pénale. Parmi les infractions commises en réseaux la pédophilie reste l'une des plus saisissantes.

A cet égard, le Nouveau Code pénal réprime à coup d'emprisonnement et d'amendes lourdes la mise en réseau d'images pédophiles, à titre privatif ou à titre commercial.

L'article 227-23 du Nouveau Code pénal punit de trois ans d'emprisonnement et de 45 000 euros d'amende le fait de fixer, enregistrer ou transmettre, en vue d'une diffusion, l'image d'un mineur lorsque celle-ci présente un caractère pornographique. Les peines sont portées à cinq ans d'emprisonnement et de 75 000 euros d'amende lorsqu'un réseau de télécommunication a été utilisé pour cela. Par conséquent, cette disposition désigne la pédopornographie par Internet. C'est sur le fondement de cet article 227-23 NCP que les dirigeants de deux fournisseurs d'accès Internet (FAI), Worldnet et Francenet, ont été mis en examen pour diffusion d'images à caractère pédophile le 7 mai 1996. Il était reproché à ces deux FAI d'avoir mis à la disposition de leurs abonnés des messages contenant des images à caractère pédophile.

En marge de cette affaire qui était toujours en phase d'instruction en 1998, la Chambre correctionnelle du Tribunal de grande instance du Mans s'est prononcée sur un cas d'achat d'images à caractère pédophile le 16 février 1998[84]. En l'espèce M. Philippe H. qui était directeur de cabinet d'un Président d'un Conseil Général s'est servi du matériel informatique dudit Conseil pour recevoir et entreposer de nombreuses images à caractère pédophile. Il a dépensé à cette fin une somme de 5610 F. A la lecture des faits, il ressort qu'il y a eu également abus de confiance prévu à l'article 321-1 du Nouveau Code pénal. Le Tribunal a condamné M. Philippe H. à 6 mois de prison dont 3 assortis de sursis pour recel d'image à caractère pédophile.

En outre, la loi relative à l'autorité parentale du 4 mars 2002 punit de deux ans d'emprisonnement et de 30 000 euros d'amende le seul fait de détenir ce type d'image. Le fait

[84] 16 février 1998, TGI du Mans, aff. Monsieur le Procureur c/ Philippe H.

de garder dans sa boîte d'e-mails en fichier attaché une image qui tombe sous le coup de cette loi est une détention d'image au même titre qu'une cassette vidéo.

Par ailleurs, l'article 227-24 du Nouveau Code pénal punit de trois ans d'emprisonnement et de 75 000 euros d'amende le fait de fabriquer, transporter, diffuser ou de faire commerce d'un message à caractère violent ou pornographique susceptible d'être vu ou perçu par un mineur. Cela revient à dire que tout responsable de site de pédopornographie est en infraction au regard de la législation française. Il en est de même pour toute personne qui télécharge pour son usage personnel, ou qui transmet à un tiers une image de pédopornographie. La Cour d'appel de Paris a jugé dans une affaire que l'infraction est susceptible d'être constituée dès lors que la fabrication, le transport ou la diffusion d'un message à caractère pornographique est susceptible d'être vu ou perçu par un mineur. Les moyens de réalisation du délit et le support du message sont indifférents à sa constitution. C'est ce que précise le juge par les termes : *«quelque moyen que ce soit et quel qu'en soit le support»* (Voir Paris, 14 déc. 1994 : Dr. Pénal 1995). Cet arrêt a l'avantage d'une interprétation large qui couvre tous les moyens du délit visé à l'article 227-24 NCP et, par conséquent, les réseaux numériques (l'Internet par exemple). Le fait de soumettre un mineur à des images violentes ou pornographiques -les deux vont aussi ensemble et le juge apprécie au cas par cas- sur le Net constitue un délit en vertu de l'article 227-24 NCP.

Le caractère de certains films qui retracent des faits constituant des crimes contre l'humanité à l'instar de la traite négrière, la Choa …semble les placer dans les infractions visées à l'article 227-24 NCP. Mais c'est très ambigu, car quand bien même l'atteinte à la dignité de la personne est frappante, le devoir de mémoire est souvent la justification de toutes ces images qui ne sont pas si rares, pas si inconnues des mineurs. Ces mots d'Adorno indiquent peut-être notre choix, dictent peut-être notre devoir : *«Il faut qu'un nouvel impératif catégorique s'impose : penser et agir de telle sorte que Auschwitz ne se répète plus».* A partir de quelle limite une image devient-elle illicite ?

La CNIL dans son dernier rapport s'est préoccupée de l'accès des mineurs à l'Internet. Elle reconnaît que « l'utilisation de l'Internet par les enfants constitue indéniablement une source

de préoccupation pour les parents et les éducateurs, conscients des dangers auxquels leurs enfants peuvent être confrontés sur le réseau du fait des contenus qui peuvent être illégaux ou de nature à les troubler (pornographie, racisme, violence physique ou psychologique), de l'existence de messageries (avec la possibilité de contacts directs avec des tiers virtuels) ou du caractère marchand et commercial des sites »[85]. La CNIL a, par la même occasion, mis un accent sur la délinquance des mineurs sur Internet. En effet, la cybercriminalité n'a pas d'âge. C'est ainsi que la CNIL a pu noter l'utilisation de l'Internet pour obtenir de manière déloyale des informations sur eux ou leurs proches.

Peu importent les motivations de ces mineurs, les préjudices nés de l'atteinte à la vie privée et l'infraction nées du stockage de données illicites restent les mêmes. Seuls les auteurs changent et pas les infractions. C'est pourquoi dans son rapport adopté le 12 juin 2001, la CNIL a manifesté son souhait de « prendre position » sur la collecte de données personnelles auprès des mineurs via Internet. Partant de ce constat, la CNIL a formulé une série de recommandations. Elle conseille, entre autre, aux sites qui désirent entretenir des contacts avec les jeunes de se servir d'une lettre d'information pour collecter l'adresse électronique et l'âge du mineur. La CNIL incite également les acteurs de l'Internet à une œuvre de pédagogie à l'endroit des mineurs. En témoigne les trois journées de sensibilisation qui a eu lieu les 22, 23, 24 mars 2002 à l'occasion de la fête de l'Internet.

L'illicéité du contenu des données diffusées sur Internet constitue l'objet d'une jurisprudence particulièrement récente et grandissante. Hormis la pédophilie, les juridictions françaises ont eu, entre 1996 et 2002, à se prononcer sur une vingtaine d'affaires particulièrement repoussantes. Les voies de recours ne sont pas épuisées dans bon nombre de cas. Le nombre des plaintes ne cesse d'augmenter. Sans dresser une liste exhaustive de ces affaires, on peut noter le racisme[86], le révisionnisme (voir Ch. Corr., TGI Paris, aff. Proc. Rép, UNADIF, FNDIR et autres c/Robert F. 13/11/1998; Référé, TGI Paris, aff. UEJF et Licra c/Yahoo ! Inc. et Yahoo France, 22/05/2000 et CA Paris, 11e ch, aff. UEJF c/Multimania Production, 21/05/2002). On note également pour la plupart du temps la contrefaçon[87] qui est malheureusement le délit au quotidien par Internet, la diffamation (voir Référé, TGI PARIS,

[85] CNIL, 22e rapport d'activité 2001, éd. 2002, La documentation Française, pp.93-96
[86] Cass., crim., aff. Ministère public et associations antiracistes contre Jean-Louis C., 21/03/2000.
Voir également TGI, Strasbourg, aff. Infoniec/Monsieur X, http://www.legalis.net
[87] Référé, TGI Paris, aff. SARL One Tel c/SA Multimania, 20/09/00, consultable sous : http//www.juriscom.net

aff. SA Free). Le 24 mai 2002, un internaute a été condamné par le TGI de Paris, à quatre mois de prison avec sursis et 20 000 euros de dommages et intérêts pour avoir envoyé en une nuit plus de 300 000 e-mails vers les serveurs de mails de Noos, les bloquant ainsi pendant près de 10 heures. Il a été condamné sur le fondement du délit d'entrave au fonctionnement d'un système de traitement automatisé de données (article 323-2 du code pénal)[88]. Le site de Paris en ligne "Kipari.com" domicilié dans l'état du New Jersey, aux Etats-Unis mais accessible aux internautes français fait actuellement l'objet d'une information judiciaire pour "loterie illicite". La législation française interdisant la pratique des paris en ligne mais cette pratique est tout à fait légale aux Etats Unis. Le conflit de législations peut encore une fois empêcher le juge français d'aller au bout de sa mission. Il se contentera d'imposer le filtrage, pour le meilleur. Mais la légalisation des cybercasinos n'ouvre-t-elle pas la voie au blanchiment des fonds provenant de ces activités de 'book maker' ?

Le cryptage que nous avons abordé comme moyen de sécurité peut facilement servir des causes dévoyées ou criminelles. Dans quelles conditions les pouvoirs publics briseraient l'impunité ?

Effectivement, le cryptage qui est un instrument de sécurité ne saurait profiter à la cybercriminalité. Le cryptage permet l'échange inaperçu de données répréhensibles sur Internet. Les hypothèses sont multiples et on note des EDI entre terroristes ou blanchisseurs d'argent et trafiquants. Selon une dépêche du journal Le Monde du 23 mars 2000, le responsable de la lutte contre la drogue au sein du gouvernement britannique a révélé que ses services ont identifié plus de mille cent (1100) sites qui vendent des drogues variées.

A l'instar de la presse, la doctrine s'est beaucoup interrogée sur la question. La réponse attendue est naturellement celle de la loi.

La convention du 19 septembre 2001 apporte une réponse : la réglementation du cryptage s'avère nécessaire pour lutter contre la cybercriminalité.

[88] Consultable sous http://www.njuris.com/breves/brev_0602.htm#br_4

Déjà, en 1996, les pouvoirs publics français avaient décidé de n'admettre le cryptage de données que jusqu'à 40 bits. L'usage de cryptages plus complexes était soumis au dépôt des clés de chiffrement chez un tiers de confiance.

La loi relative à la sécurité quotidienne (LSQ) 15 novembre 2001[89] qui modifie le Code de procédure pénale et permet aux juridictions d'instruction, de jugement, et au Procureur de la République, de désigner toute personne physique ou morale qualifiée, en vue d'effectuer des opérations techniques permettant d'obtenir la version en clair de données saisies dans une affaire. En outre, le législateur a prévu des sanctions pénales particulièrement lourdes pour les prestataires qui refuseraient de remettre la clef secrète de déchiffrement aux autorités judiciaires.

c-La cybersurveillance contre la fraude informatique

L'enregistrement ou la conservation illicite d'informations nominatives constitue une fraude au regard du Nouveau Code pénal.

Les articles 226-18, 226-19 et 226-20 du Code pénal sanctionnent ces agissements frauduleux. Dans ces trois hypothèses, le législateur a voulu sanctionner le fait d'obtenir frauduleusement des informations ou de les conserver frauduleusement. Dans les deux cas (obtention et conservation), la notion de fraude semble fort déterminante.

Ces infractions rattrapent des comportements multiples et parfois de pure négligence que les exemples suivants tirés de la pratique et de la jurisprudence nous permettront de mieux saisir :

-le fait d'obtenir des informations de manière déloyale pour les réunir, par exemple par le biais de questionnaires téléphoniques supposés anodins, ou des enquêtes.

-le fait de procéder à une collecte interdite de renseignements, en raison de leur nature. L'infraction sera constituée lorsque, en l'absence d'accord express de l'intéressé, des données sensibles, faisant apparaître les origines raciales, les opinions politiques ou religieuses, les

[89]Loi n°2001-1062 du 15 novembre 2001, J.O du 16 novembre 2001 page 18215

mœurs d'une personne ou des infractions qu'elle aurait pu commettre ou dont elle aurait connaissance seront acquises[90]. C'est le cas d'une collecte d'informations nominatives grâce à la corruption. En l'espèce, il y a eu condamnation d'une entreprise qui soudoyait les employés d'une autre société.

-le fait de conserver en mémoire des informations nominatives, au-delà de la durée prévue dans la déclaration initiale à la CNIL.

D'autre part, le délit de création de fichiers clandestins est une infraction très fréquente.

d- La cybersurveillance contre la création de fichiers clandestins

La difficulté autour de cette infraction réside dans le fait qu'elle est souvent matérielle et pas toujours intentionnelle. Hélas! bien souvent, une bonne partie des gens qui traitent des données nominatives « ignorent la loi ».La création de fichiers clandestins est un délit au terme de l'article 226-16 du Nouveau Code pénal. L'infraction est constituée dès lors que les fichiers sont réalisés sans déclaration préalable auprès de la CNIL, comme l'impose la loi. Il faut noter que le fait que les données soient sensibles ou confidentielles n'exonère pas des obligations de l'article 226-16 NCP, bien au contraire. Un professionnel ne peut sous prétexte d'être soumis au secret professionnel se soustraire à l'obligation de déclaration préalable auprès de la CNIL.

Le fait, y compris par négligence, de procéder ou de faire procéder à des traitements automatisés d'informations nominatives, sans qu'aient été respectées les formalités préalables à leur mise en œuvre prévues par la loi, est sanctionné pénalement par des peines de trois ans d'emprisonnement et 300000 Francs d'amende. Les agissements qui sont visés par cette disposition, sont relatifs à la création de fichiers clandestins. Le fait que le contenu du fichier ne porte pas manifestement atteinte aux libertés est indifférent à la qualification ; d'ailleurs, le simple fait pour une personne d'être citée directement dans ces fichiers clandestins est considéré comme un préjudice personnel et direct, fondant son action civile[91].

[90] T. corr*. Paris, 16 décembre 1994
[91] Paris, 13 septembre 1995

Ces cas sont encore nombreux. L'hypothèse déclanchant la poursuite est celle d'un contrôle ou d'une cybersurveillance qui débouche sur la découverte des fichiers non déclarés. La cybersurveillance, administrative ou judiciaire, aurait-t-elle l'avantage d'inciter à la déclaration ?

La prise en compte de la vidéosurveillance comme mode de cybersurveillance ne fait pas l'unanimité. Cependant, une partie de la doctrine lui reconnaît droit de cité. La fonction de la vidéosurveillance est variable selon les circonstances. Elle a pu faire le succès de Loft Story ces deux dernières années en France. La Webcam a permis de suivre via Internet la vie quotidienne des candidats de cette aventure sous vidéosurveillance permanente. La Webcam permet de capter des images et de les diffuser dans un format numérique via réseaux en temps réel.
La motivation d'un employeur qui installe des caméras sur le lieu de travail (dans son entreprise) peut être différente de celle d'un maire sur les lieux publics.
La vidéosurveillance qui peut servir la cause de la police administrative peut être aussi une garantie contre l'arbitraire dans une enquête judiciaire ou dans une intervention de forces de l'ordre placées sous secret : il s'agit de briser le mur du secret qui devient facilement un mur de l'impunité. C'est sur ce dernier aspect de la vidéosurveillance que nous nous pencherons davantage.

3- La vidéosurveillance : un dispositif de sécurité ou une garantie contre l'arbitraire ?

a- La vidéosurveillance : le dispositif contesté de police administrative

« Souriez, vous êtes filmés !» : ces mots peuvent paraître anodins ou même amusants. Ils traduisent une réalité plutôt inquiétante pour les libertés individuelles. Les premières caméras placées dans les voies publiques ont fait l'objet de vives critiques. On se souvient encore des querelles autour de la vidéosurveillance dans la ville de Levallois. Un contrat d'exploitation du réseau de vidéosurveillance qui liait la commune de Levallois à France Télécom a été mis en place par le maire Patrick BALKANY en 1990. On dénombrait pour la seule ville de Levallois 84 caméras qui filment 24h/24 tout ce qui est sur leur passage. La question du respect des libertés individuelles, notamment du respect de la vie privée s'est posée. Une autre question était de savoir ce que font les pouvoirs publics des images filmées qui sont aussi des données personnelles. Ce sont les données personnelles par excellence. La portée du débat expliquerait la

dissidence au sein du Conseil municipal lors en 1995, lors des élections. C'est ainsi que M. Philippe WAJNGLAS, premier adjoint au maire avait signé la pétition contre la vidéosurveillance lancée avant les élections de 1995 par le collectif *« Souriez, vous êtes filmés ! »*[92]. Avant cette divergence qui peut recevoir une interprétation politique, le juge administratif s'est déjà prononcé en 1990 en annulant la délibération d'un conseil municipal au motif qu'elle approuve la création d'un système de vidéosurveillance. Selon le juge français, l'installation généralisée et le fonctionnement permanent de caméras portaient une atteinte excessive aux libertés individuelles, et notamment au droit à la vie privée et à l'image. En l'espèce, cette mesure ne se justifiait pas par des circonstances exceptionnelles, autrement dit, par les nécessités de l'ordre public, la constatation ponctuelle d'infractions au code de la route ou d'atteinte aux personnes ou aux biens.

Le Maire qui est le garant de la police administrative au sein de la commune[93] et le responsable de la vidéosurveillance à la Police municipale de Levallois précisent que les caméras ont pour but de garantir la sécurité des personnes et des biens à Levallois. La question de la légalité de ce moyen de police administrative est posée. Le législateur et le Conseil constitutionnel se sont prononcés.

Aussi, suite à une décision du conseil municipal prise le 24/04/2000, la ville de Lyon s'est équipée d'un système de vidéosurveillance d'une importance sans précédent pour une agglomération de cette taille en France. Ce projet a été mis en oeuvre sans aucune publicité. C'était un accord politique dénué de débat de fond et de bilan des villes déjà équipées et consultation limitée niveau du Conseil municipal. Ce dispositif est capable de zoomer sur des personnes pour obtenir une photo d'identité à 100 m de distance. Ce réseau est relié à un PC municipal qui visionne et enregistre 24h/24 les images des axes les plus commerçants de la ville, les grandes places publiques et les bâtiments emblématiques de la ville comme l'Hôtel de Ville, l'Opéra, la Chambre de commerce,...ainsi que les bâtiments d'utilité publique comme l'ANPE et la poste. De plus, il est complété par la présence de caméras dans les transports en commun lyonnais (bus, métro et tram) : c'est un véritable maillage de la ville qui s'est mis en place, capable de surveiller une personne dans ses déplacements, ses achats, ses activités militantes.[94]

---

[92] « Souriez, vous êtes filmés ! » est un collectif de lutte contre la vidéosurveillance né à Levallois en 1995
[93] Voir l'article L 131-2 du Code des communes
[94] http://www.chez.com/nonabigbrother/doc.htm#awards

Le cadre juridique de la vidéosurveillance est défini par l'article 10 de la loi du 21 janvier 1995 d'orientation et de programmation relative à la sécurité (Loi 95-73 du 21 Janvier 1995). Les dispositions de cet article prévoient que l'installation des dispositifs de vidéosurveillance sur la voie publique ou dans les lieux ouverts au public et particulièrement exposés à des risques d'agression ou de vol est soumise à une autorisation préfectorale préalable délivrée après avis d'une commission départementale présidée par un magistrat du siège ou un magistrat honoraire. Les systèmes de vidéosurveillance liés à un fichier nominatif relèvent, quant à eux, de la compétence de la Commission nationale de l'informatique et des libertés (CNIL).

Le Conseil constitutionnel considère que *« pour répondre aux **objectifs** de **valeur constitutionnelle** de préservation de l'ordre public, le législateur pouvait habiliter le représentant de l'Etat dans le département et, à Paris, le préfet de police à autoriser l'installation de systèmes de vidéosurveillance assurant la transmission et l'enregistrement d'images prises sur la voie publique mis en oeuvre par les autorités publiques compétentes aux fins " d'assurer la protection des bâtiments et installations publiques et de leurs abords, la sauvegarde des installations utiles à la défense nationale, la régulation du trafic routier, la constatation des infractions aux règles de la circulation ou la prévention des atteintes à la sécurité des personnes et des biens dans des lieux particulièrement exposés aux risques d'agression ou de vol " ; qu'il pouvait également habiliter ces autorités à autoriser de telles opérations de vidéosurveillance dans des lieux et établissements ouverts au public particulièrement exposés à des dangers d'agression ou de vol afin d'y assurer la sécurité des personnes et des biens ; que toutefois la mise en oeuvre de tels systèmes de surveillance doit être assortie de garanties de nature à sauvegarder l'exercice des libertés individuelles ci-dessus mentionnées »*[95].

Le fait que la sécurité, comme nous l'avons souligné plus haut, soit un élément déterminant dans la définition de l'ordre public peut expliquer la position du Conseil constitutionnel mais ne change pas l'avis des associations qui attaquent de front la vidéosurveillance. Entre le 6 et le 9 juin 2002 plusieurs manifestations anti-vidéosurveillance ont eu lieu à travers la France (Levallois-Perret, Lyon, Vaulx-en-Velin…). Les manifestants, à cette occasion, ont eu des

[95] CC, DC 94-352 du 18 janvier 1995 relative à la Loi d'orientation et de programmation relative à la sécurité, http://www.conseil-constitutionnel.fr/decision/1999/99421/ovc.htm

mots durs envers la vidéosurveillance. Une banderole de tête était particulièrement saisissante à Vaulx-en-Velin : *« LA VIDEOSURVEILLANCE LE TOTALITARISME A PORTEE DE ZOOM »*.

Au-delà des manifestations urbaines, un débat de font reste ouvert. L'un des membres de la coordination nationale contre la vidéosurveillance rassemblée le 10 juin 2001 pour distribuer des tracts aux automobilistes à la porte de Champerret s'est confié à un journaliste : *« Nous nous inquiétons des dérives liées à la surveillance et au voyeurisme. Il y a un vrai débat à mener sur ce que devient la vie privée »*[96]. Comment protéger la vie privée dans un environnement sous surveillance ? Comment assurer la confidentialité des relations entre un avocat et ses clients alors que tous les aller et venir de ces derniers au cabinet de l'avocat sont filmés ?

Que devient le privilège de confidentialité alors que des images claires qui sont des preuves difficilement réfutables de tractations confidentielles sont aux mains des pouvoirs publics ? Des coïncidences peuvent altérer la véracité des faits filmés au dépens du professionnel tenu au secret et son client. Là, non seulement le secret est brisé mais surtout la vérité disparaît avec.

L'hypothèse d'espionnage est parfois soulevée dans le cadre privé des entreprises. Comment distinguer l'espionnage de la cybersurveillance ?

b- La vidéosurveillance et les tentations de l'espionnage dans les espaces privées

La vidéosurveillance est souvent présentée comme un dispositif sécuritaire mais à mesure que l'on se propose d'analyser la vidéosurveillance, on découvre des réalités bien plus distinctes. Aujourd'hui, les entreprises captent les moindres faits et gestes de leurs clients et salariés grâce à la vidéosurveillance et sa version électronique qu'est la Webcam.

Il est fréquent aujourd'hui travailler sous caméras. Cela semble rentrer dans les mœurs en France. La présence de ces appareils dans les entreprises est présentée comme une condition de sécurité (prévention contre le vol dans les magasins, certains incidents etc.). Il suffit pour s'en convaincre de rentrer dans un centre commercial ou un hypermarché : présentées sous forme de boules noires

[96] Parisien du 11 juin 2001, *Manifestation anti-vidéosurveillance LEVALLOIS-PERRET*

ou sous leur forme normale, plusieurs caméras placées un peu partout vous filment. Ces caméras sont reliées PC sécurité relié à un poste de police de proximité. Un tel dispositif ne peut qu'avoir un effet dissuasif auprès d'un individu malintentionné. Encore faut-il qu'il en connaisse la présence. Ces caméras sont souvent cachées. Or le fait de cacher une caméra laisse supposer une intention de surprendre. Comment nommer le fait de filmer en cachette en vue de faire la preuve d'une infraction ou mauvais geste non reconnu par la loi si ce n'est 'traquer' ?

De la même façon, une caméra peut servir à surveiller un salarié ou un groupe de salariés. Même dans une hypothèse où l'on estime que la confiance n'exclut pas le contrôle, la suspicion n'est pas de nature à garantir une bonne ambiance dans une entreprise. Quel serait donc le sentiment d'un salarié, juridiquement libre, de savoir qu'il est particulièrement suivi par la caméra de façon permanente dans ces moindres faits et gestes ?
Il arrive qu'un employeur indélicat place par manque de confiance des caméras dans les dans les salles de repos, les vestiaires, les toilettes en vue d'établir la preuve de vols etc. D'ailleurs, la Chambre sociale, dans un arrêt récent (Soc. 31 janv. 2001, n° 98-44-290), précise que le principe général de transparence n'est pas requis pour les locaux où les salariés ne travaillent pas. Un employeur avait installé des caméras dans un entrepôt de marchandises, dans lequel aucun salarié ne travaillait. Cette vidéosurveillance permet de détecter la participation d'un salarié à de multiples vols. L'intéressé est immédiatement licencié pour faute lourde, mesure dont il conteste le bien fondé.

Selon lui, la vidéosurveillance ne pouvait, dans le cas d'espèce, constituer un moyen de preuve conditionnant le licenciement, dès lors que ni le comité d'entreprise, ni les salariés n'avaient été informés de la mise en place de caméras dans cet entrepôt. Argument rejeté par la Cour de cassation, qui souligne l'absence de poste de travail dans ce local : «Et attendu que la Cour d'appel, ayant constaté que le système de vidéosurveillance avait été installé par l'employeur dans un entrepôt de marchandises et qu'il n'enregistrait pas l'activité de salariés affectés à un poste de travail déterminé, a pu retenir, à l'appui de sa décision, ce moyen de preuve ».
Enfin, des caméras partout, un simple égarement (une petite pause ou tout autre geste de l'employé non souhaité par le patron…) qui aurait pu passer inaperçu peut coûter cher à un salarié malheureux. Dans les circonstances où l'usage des caméras n'est plus motivé par la

sécurité des personnes et des biens au sein de l'entreprise, mais plutôt par la défiance et la suspicion à l'égard des collaborateurs, on se place davantage dans l'hypothèse de l'espionnage.

En revanche, il faut se garder de tout manichéisme car le bilan global de la présence des caméras dans les espaces publics et privés n'est pas négatif à tous égards. La présence de ces engins peut parfois s'avérer salutaire et ce au mépris de secrets vraisemblablement dévoyés (collusion etc.).

c-Le secret d'instruction et secret de policiers sous la caméra : une garantie contre l'arbitraire

Le secret professionnel, tout en constituant une caractéristique intrinsèque du processus judiciaire criminel, relève également du régime de protection de la vie privée, de l'honneur et de la réputation. L'instruction pénale se place sous le sceau du secret professionnel auquel le magistrat lui-même est soumis. La nature d'une enquête judiciaire explique que les agents de la police puissent observer le secret professionnel. Cependant, dans certaines hypothèses, l'intérêt du secret s'étiole face à la nécessité de clarté et de vérité. Là, la lumière des caméras est la bien venue. Cela expliquerait peut-être la réaction du législateur qui a prévu l'enregistrement audiovisuel dans la procédure pénale.

La loi du 15 juin 2000 encore appelée la 'loi Guigou' prévoit dans son article 4 l'enregistrement audiovisuel dans le processus de garde à vue de mineur[97]. Autrement dit, les déclarations des personnes mineures gardées à vue devront faire l'objet d'un enregistrement audiovisuel. Ces enregistrements ne pourront être visionnés qu'avant l'audience de jugement,

[97] L'article 4 de l'ordonnance no 45-174 du 2 février 1945 relative à l'enfance délinquante est complété par un VI ainsi rédigé : «VI. - Les interrogatoires des mineurs placés en garde à vue visés à l'article 64 du code de procédure pénale font l'objet d'un enregistrement audiovisuel.

L'enregistrement original est placé sous scellés et sa copie est versée au dossier.

L'enregistrement ne peut être visionné qu'avant l'audience de jugement, en cas de contestation du contenu du procès-verbal d'interrogatoire, sur décision, selon le cas, du juge d'instruction ou du juge des enfants saisi par l'une des parties. Les huit derniers alinéas de l'article 114 ne sont pas applicables.

Le fait, pour toute personne, de diffuser un enregistrement original ou une copie réalisée en application du présent article est puni d'un an d'emprisonnement et de 15000 euros d'amende.

A l'expiration d'un délai de cinq ans à compter de la date de l'extinction de l'action publique, l'enregistrement original et sa copie sont détruits dans le délai d'un mois.

en cas de contestation du contenu du procès-verbal de police (art. 14 de la loi, art. 4-VI de l'ordonnance n° 45-174 du 2 février 1945 relatif à l'enfance délinquante).

La volonté expresse du législateur de garantir la confidentialité de ces enregistrements mène à s'interroger sur l'intégrité du secret professionnel face à l'enregistrement audiovisuel (composé de vidéosurveillance et d'enregistrement des paroles prononcées). Tant que les données enregistrées ne sont pas divulguées aux tiers ou une personne non autorisée, il n'y a pas violation du secret d'instruction. (Le juge en fonction des circonstances peut au besoin conclure du respect de la confidentialité des données. Il peut être utile de noter que l'officier de police judiciaire a pour mission de réunir les éléments nécessaires à la décision du juge).

L'intervention des forces de l'ordre n'est pas toujours conforme aux lois. Ce qui constitue en soi une menace à l'ordre public et à l'Etat de droit. La vidéosurveillance qui permet d'établir la vérité ne devient-elle pas une garantie contre l'arbitraire ?

Des exactions policières sont parfois reconnues par la justice grâce à la vidéosurveillance. La parole des victimes, avec ou sans témoins, n'est pas d'une grande valeur probatoire face à la version d'un agent public assermenté. Les exemples en sont multiples.
L'affaire « Rodney KING » reste un exemple éloquent de violences policières filmées aux USA[98]. La caméra de Georges HOLLIDAY, un particulier qui a pu filmer les scènes, était l'ancre de salut pour la victime.
On se souvient de cet Américain de race noire rossé par un groupe de policiers en Californie, lors d'un contrôle routier le 3 mars 1991. Le 29 avril 1992, le premier jury[99] a acquitté les quatre policiers. Cette décision a provoqué des émeutes qui feront officiellement 59 morts, 2 300 blessés et près d'un milliard de dollars de dégâts. Les policiers seront inculpés à nouveau le 5 août suivant pour violation de droits civiques. Le 4 août 1993, un jury fédéral a condamné deux des quatre policiers à deux an et demi (30 mois) de prison pour violences. R. KING a eu droit à des dommages et intérêts de 3,8 millions de dollars, par une décision du 20 avril 1994.

[98] Consultable sous http : //canada.justice.qc.ca/fr/dept/pub/hmv/hate_ 35.html
[99] Le premier jury était composé de personnes de race blanche uniquement, contrairement au deuxième qui était mixte

Une lecture du Rapport de la Fédération Internationale des Droits de l'Homme sur le Brésil publié en 2000 serait d'un intérêt particulier[100]. La vidéosurveillance est gage de crédibilité et constitue une preuve irréfutable face au secret 'suspect' de policiers qu'on peut nommer à juste titre 'collusion'. Des scènes de torture ont été filmées tant par des caméras privées que par des cameras publiques. On penserait volontiers à la caméra de journaliste (souvent confisquées par les auteurs de ces exactions pour secret d'Etat ou autres selon les cas). Cependant, il faut nuancer les situations : si la vidéosurveillance implique l'usage de caméra, tout usage de caméra n'est pas de la vidéosurveillance.

La presse fait état d'un délit de salle gueule imputé aux agents de police en France ces temps-ci. Plusieurs agressions contre des policiers ont été signalées : jets de parpaing, coups de feu, des traitements tout aussi inhumains et dégradants, (et le mot 'dégradant' mérite une considération particulière à cet égard). Or, l'Amnesty international estime pour sa part que la police française est une police violente. Au journal télévisé (sur France 3), le 9 août 2002, la Ligue française des droits de l'homme présentait une victime d'une exaction policière, d'une cinquantaine d'année, certificat médical à l'appui. La jurisprudence des bavures policières pèse de plus en plus lourd. Et quand on se souvient des personnes décédées pendant une arrestation ou une garde-à-vue, on ne ménagerait aucune peine à inventer des témoins crédibles de toutes sortes, tant dans l'univers clos de la police que sur tout son passage. La caméra reste pour une partie de la doctrine une solution fiable. Plusieurs affaires récentes sont en cours d'instruction en France.
Aussi, la vidéosurveillance peut-elle être une garantie contre des témoignages calomnieux dont se plaignent parfois les forces de l'ordre.

En effet, quand on connaît toutes ces réalités, deux mots viennent souvent à l'esprit : *« Surveiller et punir»*[101].

[100]FIDH, « Rapport de position Brésil graves violations de droits l'Homme en rurale », Consultable sous http//:www.fidh.org
[101]Michel FOUCAULT, Surveiller et punir, Paris : Gallimard, 1975
Il est question d'établir les présences et les absences, de savoir où et comment retrouver les individus, d'instaurer les communications utiles, d'interrompre les autres, de pouvoir à chaque instant surveiller la conduite de chacun, l'apprécier, la sanctionner, mesurer les qualités ou les mérites. Procédure donc, pour connaître, pour identifier et pour punir au besoin : voilà la vidéosurveillance !

Les écoutes téléphoniques constituent une autre forme de cybersurveillance comme l'ont souligné la plupart des auteurs qui ont étudié la question. Les écoutes téléphoniques dès leur origine ont fait l'objet d'une perception négative. Cela n'a en rien empêché qu'elles se pérennisent et qu'elles soient légales dans certaines circonstances. Comment peut-on l'expliquer ?

4- Les écoutes téléphoniques : entre l'espionnage et l'enquête judiciaire

Deux aspects des écoutes seront analysés dans les lignes suivantes : les écoutes téléphoniques qui constituent une atteinte grave et sournoise de part leur nature à l'intimité et à la vie privée peuvent répondre à un besoin d'espionnage. On peut dans cette hypothèse parler d'un cyberespionnage (a). Elles peuvent toutefois s'avérer tout à fait légales et c'est le cas des écoutes administratives et judiciaires (b).

a- Les écoutes téléphoniques ou 'cyberespionnage' ?

Par la loi du 29 décembre 1990 sur la réglementation des télécommunications, le législateur français entendait soulever la nécessité de légiférer sur les écoutes téléphoniques qui n'avaient pas vraiment de base légale ou alors des bases fragiles. Une fois de plus, la protection des libertés individuelles s'avère indispensable.

Les écoutent qui reposaient sur des raisons d'Etat effacèrent d'un geste insolite le droit au respect de la vie privée prévu par l'article 9 du Code civil. Elles ont souvent été citées comme un outil de renseignement d'Etat pendant la Guerre froide. Une provenance, une liaison, ou un métier était une raison valable pour être mis sur écoute. Cette forme d'écoutes téléphoniques qui consiste à enregistrer ou tout simplement à accéder, frauduleusement, les données d'une correspondance téléphonique en vue d'une exploitation éventuelle.

Les auteurs de ces écoutes illégales sont de plus en plus des particuliers qui installent des tables d'écoutes sur des lignes privées. On peut indexer les détectives privés ou les concurrents déloyaux à titre d'exemple. La 'guerre industrielle' que se livrent parfois les sociétés sur des marchés concurrents est aussi une raison de ces écoutes illégales. Elles ont pour but de surprendre

les secrets de fabrication des concurrents. Rappelons qu'avec l'article 236 de la loi n° 92-1336 du 16 décembre 1992, un délit de violation du secret de fabrique en général trouve sa place dans le code du travail. Précédemment, seule la communication par le directeur, le commis ou l'ouvrier de fabrique "des secrets de la fabrique où il est employé" était punissable (ancien art. 418 du code pénal, abrogé par la loi n° 92-597 du 1er juillet 1992 et repris sous l'article L. 621-1 du code de la propriété intellectuelle, modifié par la loi du 16 décembre 1992).

On parlera d'écoutes « sauvages »[102] en évoquant ces écoutent illégales et clandestines.

Ces écoutes « sauvages » constituent un délit en vertu de l'article 226-1 du Nouveau Code pénal. C'est une loi du 17 juillet 1970 relative au respect de la vie privée qui a introduit cet article dans le Code pénal (anc. Art. 368). L'article 226-1 NCP punit d'un an d'emprisonnement et de 300 000 F d'amende le fait de porter volontairement atteinte à l'intimité de la vie privée d'autrui en écoutant, enregistrant ou transmettant des conversations téléphoniques faites « à titre privé ou confidentiel ». Les moyens mis en œuvre sont indifférents à la constitution du délit à la lecture dudit article. Cependant, un arrêté du 9 mai 1994 fixe une liste d'appareils conçus pour réaliser les opérations pouvant constituer cette infraction.

Par un arrêt du 7 octobre 1997, la Chambre criminelle de la Cour de cassation a décidé que *«c'est à bon droit que les juges ont retenu la culpabilité du dirigeant d'une société spécialisée dans la sécurité des personnes, des entreprises et des biens du chef de complicité d'atteintes à l'intimité de la vie privée, pour avoir fourni, à l'auteur principal, les adresses, et les numéros de téléphone des personnes à surveiller ; l'argumentation du prévenu invoquant l'absence d'atteinte à la vie privée des plaignants en raison du caractère professionnel des propos enregistrés ne peut être retenue, les branchements clandestins ayant, par leur conception, leur objet et leur durée, nécessairement conduit leur auteur à pénétrer dans la vie privée des personnes écoutées»*[103].
En l'espèce, le caractère insidieux des opérations témoigne de l'intention coupable et cette opération ne pourrait se réaliser sans atteindre la vie privée des personnes qu'elle visait. C'est la

[102] BENSOUSSAN A., Les télécoms et le droit, éd. Hermes, 1996, pp. 205
[103] Cass. crim., 7 oct. 1997, Bull. crim. n° 324

règle du jeu. Le téléphone n'établit pas de frontière entre vie privée et vie professionnelle. La voix emprunte la même voie pour exprimer les deux besoins (professionnel et privé, intime).
La pratique et la jurisprudence sur les écoutes téléphoniques illégales ou sauvages nous conduisent à deux remarques : ces écoutes relèvent, de par leurs natures et leurs modes de réalisation, plus de l'espionnage que de la surveillance.

L'amalgame entre la surveillance et l'espionnage semble être une erreur pour la raison suivante. La surveillance peut être un acte légitime de vigilance, d'attention et de contrôle comme nous avons essayé de l'expliquer supra. L'espionnage quel que soit le statut de son auteur revêt une connotation négative. Espionner c'est *« épier les actions, les discours d'autrui pour en faire un rapport ... c'est épier quelqu'un avec malveillance»*, explique le dictionnaire *Le petit Robert.* Cela explique peut-être les mots durs qui servent de synonymes au mot 'espion' (cafard, mouchard, délateur…, voir Le petit Robert). De cette remarque, les écoutes « sauvages » relèvent de la cybercriminalité et nous parlerons, volontiers, de 'cyberespionnage'.

En outre, la réalisation de ce délit n'épargne en rien les informations confidentielles qui relèvent du secret professionnel. Ainsi, du seul délit pourrait résulter deux dommages : l'atteinte à la vie privée et l'atteinte au secret professionnel. Imaginons un médecin et son patient qui est également son ami ou alors deux avocats amis et collaborateurs en ligne.

Qu'en est-il des écoutes légales ?

b- Les écoutes administratives et judiciaires

Qu'est-ce qui peut anoblir le concept des écoutes téléphoniques si ce n'est le système juridique ? Car même fautif, on a toujours droit au respect de son intimité et à la vie privée plus globalement. De fait, un soupçon ne suffit pas en soi à supprimer ce droit. D'ailleurs, dans un arrêt du 2 août 1984 concernant des écoutes effectuées par l'administration, la Cour européenne des droits de l'Homme a retenu que la pratique des écoutes en l'absence de règle juridique interne sont contraires à l'article 8 de la Convention européenne des droits de l'Homme. De surcroît, les

écoutes sont contraires à la Convention européenne des droits de l'Hommes signée à Strasbourg le 22 novembre 1984. Cette vision des choses proche de la conception jus naturaliste peut être l'objet d'un débat entre les jus naturalistes et les jus positivistes. En effet, pour les jus positivistes, et en particulier Kelsen, *« Gesetz ist Gesetz », « la loi, c'est la loi ».* A partir du moment où c'est la loi qui les prévoit, les écoutes ne constituent pas un délit mais deviennent une obligation. La loi semble ainsi justifier les écoutes. Cela rejoint également le fond de la pensée Thomas HOBBES lorsqu'il écrit : *« Auctoritas non veritas facit legem »,* c'est l'autorité et non la vérité qui fait la loi.

Les écoutes sont prévues par le législateur pour plusieurs raisons. En résumé, les écoutes légales sont des mesures d'ordre administratif ou d'ordre judiciaire.
Les écoutes administratives sont exercées dans les seuls buts de préserver la sûreté de l'Etat et de lutter contre le terrorisme. Elles s'effectuent à la demande des Ministères de l'intérieur et de la défense. En effet, c'est l'instruction générale sur la protection du secret de la Défense du 27 juillet 1966 qui prévoit ces mesures exceptionnelles. Ces écoutes sont réalisées par les agents de la police nationale, de la DST, de la DGSE et de la sécurité militaire. L'observation du secret professionnel par ces agents publics est très rigoureuse. Il faut reconnaître que le secret professionnel et le secret défense coïncident dans ce cas.
Ce sont des mesures d'exception en raison de leur caractère liberticide et attentatoire à la vie privée. La Loi Sécurité Quotidienne renforce considérablement ces mesures de lutte contre les atteintes à la sûreté intérieure et extérieure de l'Etat et le terrorisme international (voir l'amendement n° 12 de la LSQ dans les annexes)[104]. Désormais, les procédure d'audition ou d'interrogatoire *« peuvent faire l'objet d'un enregistrement audiovisuel ou sonore, les dispositions des quatrième à neuvième alinéa de l'article 706-52 sont alors applicable ».*

La pratique des écoutes par l'autorité administrative ne diffère pas de celle des espions, sauf qu'elles sont dites réalisées dans l'intérêt supérieur de la Nation et de l'Etat. C'est la suprématie de l'Etat, plus que l'intérêt général, qui fait échec à l'application de l'article 226-1 NCP. Très souvent, la vie privée résiste difficilement à la Raison d'Etat, même dans un Etat de droit. Justement, il suffit que la loi prévoie quelque chose pour qu'elle soit faisable (pour ne pas oser

[104] Consultable sous http://www.lsijolie.net/lsq

dire juste). Pascal pensait que *« ne pouvant faire ce qui est juste fût fort, on a fait que est fort fût juste »*. On peut en déduire qu'il ne suffit pas d'avoir raison, il faut avoir le droit d'avoir raison. Ca laisse songeur.

La loi n°91-646 du 10 juillet 1991 relative au secret des correspondances émises par la vois de télécommunications a posé les bases légales des écoutes téléphoniques en France. Avant cette loi, la Cour européenne des droits de l'Homme et la Cour de cassation s'opposaient quant à leurs jurisprudences sur les écoutes téléphoniques : elles sont illicites selon la Cour européenne et licites selon la Haute juridiction française. En vertu de cette loi, les écoutes légales sont les écoutes judiciaires commandées par un magistrat et des interceptions dites de sécurité autorisées par le Premier Ministre.

Le Code de procédure pénale prévoyait déjà, en l'absence d'une législation précise, les conditions des écoutes judiciaires. La Cour de cassation autorisait les écoutes judiciaires sur le fondement du Code de procédure pénale. Les articles 81 et 151 du Code de procédure pénale confèrent au juge d'instruction le pouvoir de procéder par commission rogatoire à tous les actes d'information utiles à la manifestation de la vérité. Par conséquent, il est autorisé à ordonner des écoutes téléphoniques. Les dispositions de l'article 151 du Code de procédure pénale ont été le fondement d'un arrêt de principe du 9 octobre 1980[105]. La Chambre criminelle estimait notamment que *« le placement sur écoutes d'une ligne téléphonique du domicile d'un inculpé détenu, accomplit délégation des pouvoirs du juge d'instruction, sous contrôle sans artifice ni stratégie dès lors que ce procédé n'a pas eu pour résultat de compromettre les droits de la défense ».*

Au terme de l'article 81 NCPP, *« le juge d'instruction procède, conformément à la loi à toutes les actes d'information qu'il juge utile à la manifestation de la vérité ».* La Chambre criminelle par un arrêt du 6 octobre 1999 décidait qu'*«en sollicitant régulièrement la communication d'écoutes téléphoniques et en ordonnant leur retranscription, le juge d'instruction ne fait qu'user de ses prérogatives que lui confère l'article 81 du Code de procédure pénale »*[106]. Par un autre arrêt du

[105] Cass. Crim., 9 oct. 1980: D. 1981, note Pradel.
[106] Cass. Crim., 6 oct. 1999: Bull. crim. n° 210

16 mai 2000, la même chambre de la Cour de cassation retenait qu'un juge d'instruction peut ordonner par commission rogatoire *« l'ouverture de scellés de cassettes de surveillance téléphonique saisis dans le cadre d'une autre procédure et ordonner la transcription des conversations »*[107].

Les écoutes peuvent aussi constituer une obligation légale dans certains cas. C'est le cas des professionnels de la bourse. Les conversations téléphoniques dans les sociétés de transactions boursières sont enregistrées pour servir de preuve. On peut se référer aux Règlements n° 90-12 et 90-13 du 25 juillet 1990 relatifs aux conditions d'exécution et de réception des ordres transmis par des intermédiaires professionnels.

On peut noter que les écoutes légales sont généralement pratiquées par des professionnels qui semblent être de par la nature de leurs fonctions soumis au secret professionnel. Si telle est la réalité, les écoutes légales ne constituent pas a priori une atteinte au concept du secret professionnel. En revanche, il faut noter qu'il y a 'secret professionnel et secret professionnel'. Le secret professionnel qui s'impose à des corps de professionnels disparates est-il toujours à partager ? Ne serait-il pas fabuleux d'entrevoir le partage du secret médical et du secret judiciaire ?
Apparemment, le secret professionnel ne forme pas un tout indivisible. A chaque profession correspond une parcelle de secret professionnel. Dans cette vision des choses, la pratique des écoutes légales ne peut que répondre à des conditions strictes. A chaque profession son secret. La jurisprudence de la Chambre criminelle semble avoir approche sectorielle du secret.

L'analyse de la cybersurveillance nous montre les limites de la confidentialité ou du secret professionnel à travers les archives numériques. Les enjeux autour de l'ordre public et la lutte contre la cybercriminalité semblent constituer un défi au secret professionnel. Le silence ou la discrétion du professionnel ne suffit plus à garantir le secret professionnel à l'ère numérique. Car là où la bouche se tait, l'œil, lui continue de voir. Or la contradiction entre 'secret et surveillance' est flagrante.

[107] Cass. Crim., 16 mai 2000: Bull. crim. n° 190

Il paraît difficile de garantir le secret dans un système qui surveille systématiquement ou presque systématiquement, même les sphères de la vie privée et intime. Ou bien le secret subsiste et la surveillance ne réussit pas, ou bien la surveillance aboutit et le secret disparaît. Cela nous conduit à la question suivante : peut-on concilier la cybersurveillance et le secret professionnel ou alors, la cybersurveillance constitue-t-elle une atteinte systématique au secret professionnel ?

Titre II / La cybersurveillance comme atteinte systématique au secret professionnel

Ce titre II va être traité en deux chapitres. Ce qui revient à analyser, en premier, la compatibilité de l'inviolabilité du secret professionnel avec la cybersurveillance des correspondances professionnelles (chapitre I), avant d'aborder les limites légales de la cybersurveillance : des libertés fondamentales (Chapitre II).

Chapitre I / La question de la compatibilité de l'inviolabilité du secret professionnel et la cybersurveillance des correspondances professionnelles

Il convient d'abord de soulever la question de la porosité des frontières professionnelles à laquelle conduisent la cybersurveillance et l'intervention d'intermédiaires techniques conduit-elle à un partage élargi du partage du secret professionnel ? (1) L'observation des écoutes téléphoniques mène de la violation de la vie privée à la négation du secret professionnel (2). On observera ensuite l'antinomie des concepts du secret professionnel et de la fouille des e-mails professionnels (3) pour y voir les limites du privilège de confidentialité (4).

1- <u>La porosité des frontières professionnelles</u> : un partage élargi du secret professionnel ?

a- La porosité induite par l'intervention technique

Une observation semble utile à cet égard : la technicité de la sécurisation oblige le professionnel à faire appel à un prestataire intermédiaire. Cette hypothèse est celle d'un 'ami indésirable' mais incontournable.

Ce dernier partage-t-il le secret professionnel auquel l'avocat, le médecin et le banquier sont assujettis?

La question de la soumission des intermédiaires techniques au secret professionnel s'est déjà posée. IRIS[108] a proposé de soumettre l'activité du prestataire technique d'accès, de transport, de stockage temporaire ou d'hébergement au secret professionnel. Ces intermédiaires techniques ne doivent être tenus de communiquer les éléments d'identification des utilisateurs de ses services qu'à la seule requête de l'autorité judiciaire, dans les conditions prévues par la loi. L'intermédiaire garde envers les tiers le secret le plus absolu sur ce qu'il a vu ou entendu au cours de son expertise. Il ne peut se départir du secret qu'avec l'accord des parties et si la loi le permet.

En effet, en vertu d'une loi du 29 mai 2000 relative à la liberté de communication, l'hébergeur, à l'instar du médecin ou de l'avocat sera tenu au secret professionnel. Le secret en question n'est pas partagé entre professionnels de même cabinet, même ordre etc. comme exposé supra.

Que faut-il en penser ? Ne s'agit-il pas d'une dérogation au secret professionnel plutôt que d'une extension du secret professionnel au prestataire technique ?

Au fait, la nécessité de recourir au prestataire technique justifie amplement cette dérogation au profit du professionnel (avocat, médecin ou banquier). Car en principe, en vertu de l'article 226-13 NCP, la collaboration avec un prestataire technique qui ne partage pas normalement le secret avec le professionnel est une infraction. Toutefois, le principe de la réalité fait échec à

[108] Imaginons un Réseau Internet Solidaire est une « association qui suit l'actualité de l'Internet, notamment sous l'angle judiciaire et législatif, pour favoriser le développement de l'Internet non marchand, pour qu'y soient respectées les libertés individuelles comme les libertés publiques » ; l'association Iris a été créée le 4 octobre 1997. http://www.autonomie.org/iris.htm

cette vision rigide de l'article 226-13 NCP. Si la loi du 29 mais 2000 est une solution aux incertitudes autour du partage informel du secret entre le professionnel et le prestataire technique, sa nécessité reste discutable.

L'article 226-13 NCP s'appliquerait commodément aux intermédiaires en fonction de la nature même de leurs activités qui brassent aujourd'hui non seulement des données personnelles mais surtout l'ensemble des secrets de presque tous les secteurs. La relecture dudit article est peut-être nécessaire : *« la révélation d'une information à caractère secret par une personne qui en est dépositaire soit par état ou par profession, soit en raison d'une fonction ou d'une mission temporaire, est punie d'un an d'emprisonnement et de 100 000 F (soit 15244,90 Euros) »*.[109]

La jurisprudence a récemment confirmé la soumission de l'administrateur réseaux au secret professionnel. Un arrêt de la Cour d'Appel de paris du 17 décembre 2001[110] statuant en appel du jugement du tribunal correctionnel du 2 novembre 2000 à propos de l'affaire du CNRS confirme que les e-mails constituent une correspondance privée, cependant il apporte une nuance. La Cour d'appel semble reconnaître le droit à l'administrateur réseau de filtrer les e-mails, de les contrôler et de prendre les mesures nécessaires, si cela est légitimé par des besoins de sécurité. Cependant en aucun cas l'administrateur ne serait autorisé à divulguer le contenu des messages à l'employeur.

En l'espèce, une divulgation a eu lieu, c'est pourquoi la Cour d'Appel de Paris confirme les peines prononcées en première instance. Par ailleurs, la Cour d'appel a considéré que les correspondances émises, transmises ou reçues par la voie des télécommunications ou alors le courrier électronique doit être considéré comme une correspondance privée bénéficiant à ce titre de la protection de la loi du 10 juillet 1991 sur les télécommunications.

En revanche, compte tenu des aspects particuliers de l'affaire, la Cour d'Appel a assorti ces peines du sursis et précises qu'elles ne seront pas inscrites sur leur casier judiciaire.

Il faut rester prudent quant à la portée de cet arrêt, car toutes les voies de recours ne sont pas épuisées : l'éventualité d'un pourvoi en cassation est forte en l'espèce.

---

[109] Une vision 'troperienne' reconnaîtrait à cet article toute sa validité : il faut s'en remettre à l'interprétation. Cet article qui n'énumère pas les professionnels tenus au secret peut s'appliquer à l'intermédiaire technique.

[110] La décision est publiée sur http://www.foruminternet.org/documents/jurisprudence/lire.phtml

La soumission des professionnels au secret professionnel du fait qu'il traitent du secret professionnel d'autres professionnels ne voile pas pour autant une réalité : dès lors qu'ils accèdent à des informations confidentielles dont les gardiens réguliers ne sont pas autorisés à leur donner l'atteinte au secret est consommée, ipso facto.

La cybersurveillance implique l'intervention de professionnels de secteurs différents soumis au secret professionnel dans des domaines où la déontologie requiert le secret professionnel. Mais il y a bien un problème : l'identité conceptuelle n'implique pas nécessairement une identité des réalités.

b- La porosité induite par la cybersurveillance : une obligation de transparence

La confidentialité est-elle devenue avec le numérique une confidentialité à large éventail ?
D'une part, la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés posait déjà une obligation de transparence qui s'exprime par la déclaration préalable auprès de la CNIL. Cette déclaration est obligatoire pour tout traitement automatisé des données nominatives. Cette loi interdit également que les données soient collectées de façon frauduleuse, déloyale ou illicite. Elle impose par conséquent une complète information des personnes concernées par ces données. Autrement dit, les personnes concernées par les données doivent savoir la destination des données et le lieu où s'exerce le droit d'accès et de rectification des celles-ci. Or dès lors que la loi contraint à la déclaration de données nominatives qui renferment de données confidentielles, un pas décisif est franchi.

D'autre part, la cybersurveillance, notamment dans la lutte contre la cybercriminalité et le terrorisme, implique nous l'avons remarqué plus haut l'intervention d'agents administratifs. Les cybersurveillants à la trace de délinquants et de terroristes ne peuvent qu'avoir accès à toutes les données confidentielles. Un projet de Convention du Conseil de l'Europe finalement abandonné aurait conduit à la cybersurveillance générale et permanente de tous les internautes par enregistrement a priori de leurs agissements sur Internet. Une fois transposée dans l'ordre interne,

une telle mesure mettrait fin au privilège de confidentialité. D'ailleurs, la CNIL estime dans son rapport de 2001 qu'*« une telle mesure, ayant été dans un principe aussi généralement défini, considérée comme disproportionnée dans une société démocratique »*[111].
La cybersurveillance semble être, dans ces conditions, un obstacle au caractère absolu de la confidentialité. Cela expliquerait-il la méfiance des techniciens ou travailleurs dont la déontologie prescrit le secret professionnel à l'égard de la traçabilité et de la cybersurveillance?

c- La traçabilité des données fragilise-t-elle de la confidentialité ?

Un colloque organisé le 26 avril 2000 par l'Union des Jeunes Avocats et intitulé *« L'anonymat dans la société de l'information : fichage et démocratie »* donnait à Raymond FORNI l'ex-Président de l'Assemblée Nationale qui était également vice-président de la Commission Informatique et Libertés l'opportunité d'exprimer ses inquiétudes sur les atteintes à la vie privée et la confidentialité.
A cette occasion, 'l'avocat et le politique' réclamait le droit à l'anonymat et à la confidentialité via les réseaux : *«l'homme contemporain est maintenant un individu perpétuellement repérable […] Ces dangers, vous le savez comme moi, votre colloque en est la preuve, sont, à titre principal, l'absence d'anonymat, le défaut de confidentialité du message (privé ou commercial) ; enfin, et c'est peut-être le plus grave à mes yeux, le repérage ; ce que l'on appelle d'un mot en forme de barbarisme la « traçabilité »*. Il a souligné l'utilité de la traçabilité dans les enquêtes en évoquant, entre autres, l'assassinat du Préfet ERIGNAC. Les études ont su démontrer comment le téléphone portatif repère à la dizaine de mètres près l'emplacement de son utilisateur.

Par ailleurs, notons que le traçage est inhérent à l'informatique. Le traçage des opérations sur le disque dur ou le serveur, la mémoire cache du serveur, les cookies et la messagerie constituent autant de preuves ou d'éléments révélateurs des activités informatiques. Le volet historique du navigateur qui est l'ensemble des moyens utilisés pour surfer sur le Web (Internet explorer, Nescape communicator etc.) permet d'accéder plus facilement aux sites visités, aux traces laissées après une connexion. C'est d'ailleurs ce qui permet de revenir sur des recherches dont on oublie les coordonnées. Tout est bien évident, il suffit de cliquer sur le volet historique. Le danger

[111] CNIL, Rapport 2001 déjà cité, p.179

pour la confidentialité est que ce volet n'est pas codé. Aussi, les informations recueillies peuvent permettre de connaître les habitudes de l'utilisateur du poste. Par exemple, une visite fréquente de sites de trafic de stupéfiants serait une preuve à charge dans une enquête sur usage de stupéfiants. Ce serait du moins de nature à emporter la conviction du juge.

La question devient délicate lorsqu'on est tenu au secret professionnel. Sauf à avoir effacé toutes les traces, l'accès au PC à usage professionnel ne devrait-il pas être rendu impossible aux tiers non autorisés ?

Les écoutes téléphoniques constituent de par leur nature une violation de la vie privée. Mais la question se pose de savoir si elles ne constituent pas également une négation pure et simple du secret professionnel.

2- <u>Les écoutes téléphoniques</u> : de la violation de la vie privée à la négation du secret professionnel

Contrairement aux idées reçues, les communications sur le réseau GSM ne sont pas protégées. Quoique complexe à réaliser, l'interception des communications est possible tant sur la liaison radio (GSM) que sur le lien filaire (RTC ou RNIS). Aussi, tout document envoyé par fax peut faire l'objet d'interception et d'enregistrement à l'insu des personnes impliquées dans la correspondance. Il suffit de visiter la page http://securinet.free.fr/doc-e-02.html et suivantes pour s'en convaincre.

Comment concilier les écoutes téléphoniques avec le secret professionnel ? Comment garantir la confidentialité des affaires face à des écoutes qui sont la preuve vivante de la divulgation des informations ?
La confrontation du secret professionnel à la cybersurveillance ne soulève pas systématiquement la question d'un élément intentionnel du professionnel. Car ce n'est pas lui-même qui viole le secret professionnel mais des tiers qui lui extorquent des informations dont il est gardien à titre professionnel. Dès lors que l'information est divulguée ou connue via surveillance électronique, l'atteinte au secret prévue à l'article 226-15 du Nouveau Code pénal est consommée.

Les écoutes téléphoniques sont particulièrement redoutables pour le secret professionnel dans la mesures elles ont plus de justifications mais n'ont aucune quant aux personnes écoutées. Lorsqu'une personne est mise sur écoutes, toutes les personnes avec qui elles entretient des communications téléphoniques sont logiquement écoutées (cela va de soi. On ne parle pas seul au téléphone).
La difficulté surgit lorsqu'un psychanalyste reçoit l'appel d'un patient mis sur écoutes. Les enregistrements issus d'une telle situation constituent à la fois une violation de l'intimité de la vie privée du patient et une atteinte au secret dont peut se prévaloir légitimement le médecin.
Il en est de même des communications téléphoniques effectuées entre une personne, criminelle fût-elle et son avocat. Si une enquête judiciaire justifie la mise sur écoutes du client, rien ne semble justifier la mise sur écoutes de l'avocat qui est soumis au secret professionnel. On peut en dire autant pour tout professionnel soumis au secret et ses clients ou partenaires (banquier, notaire etc.).

De ce constat, une déduction est possible : sauf à démontrer que les écoutes sont pratiquées de sortes à qu'il y a eu partage et non atteinte au secret, les écoutes téléphoniques infligées à un professionnel tenu au secret à titre principal ou secondaire (par coïncidence) porte nécessairement atteinte au secret. On ne peut pas protéger le secret professionnel en mettant le professionnel sur écoute. Même si les services d'écoutes, dans le contexte des écoutes administratives et judiciaires sont eux aussi soumis au secret professionnel, il n'y a pas de fusion de secrets professionnels. On peut même objecter : à chacun son secret.

Ainsi, les écoutes opérées dans la sphère du secret professionnel peuvent non seulement constituer une atteinte à la vie privée mais aussi une négation pure et simple du secret professionnel. Entre 'l'être' et le 'non être', il n'y a pas de conciliation possible ; il n'y a que paradoxes et contradictions. En somme, lorsque les informations confidentielles reçues à titre professionnel cessent d'être confidentielles par le biais de telles infiltrations, peut-on encore parler de secret professionnel ?
L'interception des correspondances est également perçue comme un danger au secret professionnel. Pourquoi en est-il ainsi ?

3- <u>L'interception des correspondances entre le secret professionnel et le secret d'Etat</u> : le conflit des secrets

En février 2000, des documents « top secret », récemment déclassifiés par l'Agence américaine pour la sécurité nationale (NSA), ont confirmé pour la première fois, officiellement, l'existence du programme d'espionnage dit « Echelon ». En effet, « Echelon » est un vaste système d'interception mondiale des communications téléphoniques privées, des fax et courriers électroniques. Ces données ont été obtenues par des chercheurs de l'Université George Washington, de la capitale fédérale, regroupés au sein de l'organisation National Security Archive, en vertu du Freedom Information Act (la loi sur la liberté de l'information)[112].

Le Congrès des Etats-Unis décidait en décembre 1999 d'ouverture d'une enquête préliminaire à la suite d'accusations selon lesquelles la NSA avait placé sur écoute des citoyens américains, ce qui est contraire à son statut. Cette surveillance insidieuse se ferait indirectement via l'agence de renseignement britannique, en vertu d'un accord baptisé UKUSA Alliance conclu en 1948 entre les deux pays. Or la NSA a été créée en 1952 pour *« intercepter et analyser les communications étrangères au profit du département de la Défense et pour assurer la sécurité et le codage des communications confidentielles de l'administration américaine »*[113].
James BANFORD qui est l'un des spécialistes américains de la NSA précise que la NSA emploie 38.000 personnes, soit deux fois plus que la CIA et son budget est également supérieur. Faut-il en déduire que l'interception de correspondances n'a jamais rien de légitime ?

« Echelon » qui fait appel aux technologies les plus avancées, est un élément crucial du réseau mondial qui permet l'espionnage de toutes les correspondances, privées ou commerciales, à l'échelle planétaire. Le rapport de Duncan Campbell rédigé pour le Parlement européen, documents à l'appui est particulièrement accablant. La présentation de ce rapport a suscité

[112]Ces données sont publiées sur le site Internet http://www.gwu.edu/nsarchiv de l'université George Washington
[113]AFP WASHINGTON, Le programme Echelon : les preuves, du 04/02/2000

l'ouverture d'une enquête internationale, confiée à la DST. Sous prétexte de lutte contre le terrorisme, conversations téléphoniques, fax, e-mails, sont interceptés et analysés à des fins économiques et politiques. C'est ainsi qu'Airbus a été écarté d'un marché important en Arabie Saoudite, les informations recueillies par le gouvernement américain permettant à Boeing de surenchérir et de signer le contrat. En outre, l'espionnage peut aussi porter atteinte à la vie privée et, par delà, au secret professionnel et au secret de fabrication etc., surtout avec l'essor des communications par Internet et du commerce électronique.

Dans une question écrite au Gouvernement publiée au Journal Officiel du Lundi 14 février 2000, Monsieur Georges SARRE avait attiré l'attention du Ministre des Affaires étrangères, H. VEDRINE, sur le réseau « Echelon » de surveillance et d'interception globales des télécommunications à l'échelle mondiale, géré conjointement par les États-Unis. le Royaume-Uni, le Canada, l'Australie et la Nouvelle-Zélande. Outre l'engagement de poursuites judiciaires, au civil comme au pénal, auquel la divulgation de ces documents pourrait donner lieu devant les tribunaux français, Georges SARRE estime qu'elle doit être par ailleurs l'occasion pour le Gouvernement de discuter de ce dossier avec l'ensemble de ces partenaires concernés afin d'en obtenir les explications qu'il est en droit d'attendre.

Quelle est donc la frontière entre les nécessités de police (administrative ou judiciaire), essentielle à la protection des droits de l'homme et les libertés fondamentales ?

Comme nous l'avons souligné plus haut (Titre I, chap. I, 3), ces écoutes illégales ne se limitent pas aux Etats-Unis. Pendant trois ans (entre janvier 1983 et mars 1986), des écoutes illégales ordonnées par la cellule anti-terroriste de l'Elysée ont été effectuées sur les lignes d'un journaliste, Edwy PLENEL, d'un avocat, Antoine COMTE, d'une actrice, Carole BOUQUET d'un "écrivain", Jean-Edern HALLIER et d'autres personnes. La levée du secret défense en 1998 par ordonnance du Premier ministre a permis l'instruction de cet épineux dossier dit des *« écoutes téléphoniques de l'Élysée ».*

Selon un article publié le 13 août 2002, sur le site de TF1[114], le juge VALAT vient d'ordonner le renvoi de 12 proches de François Mitterrand, mis en examen dans l'affaire des écoutes de l'Elysée, devant le tribunal correctionnel de Paris.

Le 'rideau' du secret d'Etat a permis d'assurer la pérennité de ces interceptions de télécommunications à des fins de concurrence déloyale et d'espionnage d'Etat. Or, la raison du plus fort étant la meilleure, le secret de correspondance et le secret professionnel s'éclipsent devant le secret d'Etat.

La fouille des e-mails est plus que jamais un sujet d'actualité, mais un sujet préoccupant également. Car si la fouille des e-mails devient nécessaire ou tout simplement obligatoire (parce que la loi en a ainsi décidé), elle ne semble pas conciliable avec le secret professionnel. Doit-on parler d'antinomie ?

4- <u>Le secret professionnel et la fouille des e-mails professionnels</u>: deux concepts antinomiques?

Le respect de l'intimité de la vie privée semble en appeler davantage au secret qu'à la transparence. Le respect de la vie privée correspond au droit au respect de l'intimité de la vie privée. Le secret professionnel et la transparence qui sous-tend la fouille des correspondances privées sont deux concepts contradictoires. Ce qui montre, d'emblée, la complexité du problème.

Comme nous l'avons souligné dans les premières lignes de nos travaux le secret évoque le silence, protection et mise à l'écart de l' 'intime', la discrétion pour garantir le respect de la sphère privée. Pourtant, le secret couve parfois une ambiguïté : il est aussi porteur de dissimulation, d'opacité, de clandestinité, d'obscurité, de ténèbres, de déloyauté.

[114] sous http://www.tf1.fr/news/france/0,,930278,00.html

La transparence laisse, quant à elle, transparaître avec clarté, limpidité et netteté les informations et les données que le secret professionnel aurait tenues pour confidentielles. La transparence tient la vérité pour but.

La fouille des e-mails répond-elle à une nécessité de transparence ou constitue-t-elle plutôt de l'indiscrétion au mépris du secret ?

La cybersurveillance renvoie aussi bien à l'indiscrétion au mépris du respect de la vie privée.

La transparence, en effet, c'est l'organisation a priori de l'absence de secret des correspondances. Il s'agit pour la cybersurveillance d'éliminer le secret en dégageant l'information qu'il avait pour effet de voiler. Les archives secrètes doivent être accessibles sans délai dans le cadre de cette fouille. Comment garantir le secret professionnel dans une telle hypothèse.

La fouille des e-mails n'est pas une fouille limitée ou relative. La fouille des e-mails telle que prévue par la plupart des législations dans la lutte contre le terrorisme une fouille systématique et générale. Cette observation justifie parfois des critiques à l'égard des mesures sécuritaires inspirées des événements du 11 septembre 2001.

Il suffit qu'on se propose d'analyser la fouille des e-mails telles qu'énoncée dans le RIPA et dans la Loi sécurité quotidienne pour se rendre à l'évidence qu'elle constitue par essence l'opposé de la confidentialité sur laquelle repose le secret professionnel.

Valentin LACAMBRE, fondateur d'un des plus anciens prestataires de services indépendants français, *altern.org*, voit dans la fouille des e-mails *« la fin du secret de la correspondance privée »*[115].

Entre le secret professionnel et le secret des correspondances il existe un lien ténu que la pratique ne distingue même presque pas. Si la divulgation des informations confidentielles reçues à titre professionnel constitue une atteinte au secret professionnel, la fouille des e-mails d'un professionnel astreint au secret en est une aussi.

[115]Consultable sous : infos.samizdat.net/article.php3?id_article=157

En principe, se disent antinomiques, deux lois ou deux principes qui se contredisent. 'Antinomie' vient du mot latin 'antinomia' qui signifie 'contradiction'. La contradiction est une relation entre deux propositions telle que si l'une est vraie, l'autre est nécessairement fausse. Cette vision est aussi celle de Von WRIGHT qui s'est déjà penché sur le cas où deux normes se contredisent dans le même système juridique.

Dans le langage de Kant, 'antinomie' est un conflit dialectique, c'est à dire conflit entre les lois de la raison pure. Face à ces deux logiques contradictoires que nous venons de décrire (la fouille des e-mails et le secret professionnel), il nous semble permis de parler d'antinomie.

Dans le chapitre suivant la question va se poser de savoir quelle est la limite que la loi pose à la cybersurveillance.

Chapitre II / Les libertés fondamentales comme limite légale de la cybersurveillance

Ce chapitre sera consacré à l'étude de la protection pénale des e-mails comme garantie du secret professionnel face à la cybersurveillance (1) et du droit à la vie privée comme limite de la cybersurveillance « régulière » (2). Notre analyse touchera aussi le rôle de la CNIL dans la cybersurveillance (3) pour, enfin, soulever la problématique de la présomption d'innocence confrontée à la cybersurveillance (4).

1-La protection pénale des e-mails comme garantie du secret professionnel face à la cybersurveillance

Le jugement prononcé le 02 novembre 2000 par la 17ème Chambre correctionnelle du Tribunal de grande instance de Paris pose, pour la première fois, le principe selon lequel il convient d'assimiler le courrier électronique à une correspondance privée. Aussi, en tant que tel, l'e-mail est protégé par le secret des correspondances privées prévu et réprimé par le Code Pénal. Il est précisé dans ce jugement que *« l'envoi de message de personne à personnes*

constitue de la correspondance privée […] cette relation est protégée par la loi dès lors que le contenu qu'elle véhicule est exclusivement destiné à par une personne dénommée à une autre personne également individualisée, à la différence des messages mis à la disposition du public ». Cette décision a été confirmée par la Cour d'appel de Paris. Par ailleurs, un arrêt rendu le 20 octobre 2001 par la Chambre sociale de la Cour de cassation a également consacré le caractère confidentiel et personnel du courrier électronique.

La Cour a donné par la même occasion une définition du terme de 'correspondance'. Selon la 17e Chambre correctionnelle du TGI de Paris, *« le terme de correspondance désigne toute relation par écrit existant entre deux personnes identifiables, qu'il s'agisse de lettres, de messages ou de plis fermés ou ouverts »*. Cette définition doit être nuancée, car, à première lecture, elle semble exclure les messages électroniques adressés à un groupe de personnes dans un cercle fermé de relations. Or il est fréquent qu'un individu envoie un e-mail à plusieurs personnes d'un nombre donné sans pour autant vouloir en faire un message mis à la disposition du public. C'est le procédé dit des « e-mails en chaîne ». Ils permettent à un employeur ou à un chef d'équipe de transmettre un message aux membres d'une entreprise. N'étant pas rendus publics, ces messages semblent bénéficier d'une présomption de confidentialité. Tout tiers non autorisé qui intercepte, de mauvaise foi, ce message commet l'infraction d'atteinte au secret des correspondances.

Traditionnellement, le secret s'impose en matière de correspondances (art. 226-15 et 432-9 du code pénal) et dans l'exercice certaines professions (art. 226-13 et 226-14 du code pénal). Ces infractions pouvaient dès lors permettre de sanctionner certaines indélicatesses facilitées par l'informatique : l'interception des renseignements par le biais des réseaux, la duplication d'un document confidentiel sur un ordinateur etc.

Il faut observer ici une double protection pénale pour les correspondances professionnelles : elles bénéficient à la fois d'une protection au titre du secret de correspondances (vis à vis des tiers non autorisés) et au titre du secret professionnel dans les cas où les professionnels sont tenus au secret (l'obligation de confidentialité qui s'impose au professionnel lui-même).

Le droit au respect de la vie privée qui est un droit fondamental se trouve être en général la limite que la loi pose à la cybersurveillance. Cependant cette limite ne semble concerner que la

surveillance effectuée dans un cadre privé. C'est le cas de la cybersurveillance au sein d'une entreprise.

2- <u>Le droit à la vie privée comme limite de la cybersurveillance « régulière »</u>

Les employeurs peuvent-ils légalement surveiller l'utilisation par leurs employés du courrier électronique et de l'Internet ? Si oui, dans quelles limites ?

a- La cybersurveillance des salariés et le droit au respect de la vie privée

La gestion des novelles technologies de l'information et de la communication (NTIC) va amener les entreprises à veiller à ce que les salariés n'en fassent pas un usage abusif sans lien avec leur activité professionnelle. Ainsi, il ressort d'un arrêt de la chambre sociale de la Cour de cassation du 14 mars 2000 que l'utilisation ludique des nouvelles technologies est constitutive d'une faute (faute grave en l'espèce en raison du caractère systématique des prises de paris).
Les entreprises rédigent parfois des « Chartes » sur « l'Eticnet », elles installent aussi des logiciels de contrôle minimum permettant d'éviter les abus manifestes (davantage sur la nature et la durée des connexions que sur leur contenu), et surtout permettant de sécuriser les fichiers et données de l'entreprise.

Une question se pose : comment concilier ce nécessaire et légitime contrôle avec les libertés individuelles et collectives ?
La Constitution Française de 1958 ne parle évidemment ni d'Internet ni des NTIC, mais la décision du Conseil Constitutionnel « Vidéosurveillance » du 18 janvier 1995 énonçait que *« la méconnaissance du droit à la vie privée peut être de nature à porter atteinte à la liberté individuelle énoncée à l'article 2 de la Déclaration des Droits de l'Homme de 1789 ».* Cette analyse a été confirmée par la décision (CMU)[116] du Conseil constitutionnel du 23 juillet 1999 :

[116] Cf. D. 2000 p422

« chacun a droit au respect de la vie privée ». La loi du 6 janvier 1978 appelée *« Informatique et liberté »*[117] pose le principe que l'informatique ne peut porter atteinte ni à la vie privée, ni aux libertés individuelles.

Le Doyen Ph. WACQUET[118] souligne, à juste titre, que *« la vie personnelle des salariés doit être protégée, malgré eux parfois, contre un envahissement excessif de leur vie professionnelle […] Le droit à une vie familiale normale évoqué par le Conseil d'Etat dans sa décision GISTI du 8 décembre 1978 a été proclamé pour le droit des étrangers. Mais cette règle a vocation à s'appliquer à tous, et en particulier aux salariés lorsqu'il s'agit d'établir une coupure entre le travail et la vie personnelle »*

La chambre sociale est très attentive à la loyauté qui doit présider les rapports des parties au contrat de travail : Ainsi dans l'arrêt « Néocel » du 20 novembre 1991, elle affirme que *« si l'employeur a le droit de contrôler et de surveiller l'activité de ses salariés pendant le temps de travail, tout enregistrement, quel qu'en soit les motifs, d'images ou de paroles à leur insu constitue un mode de preuve illicite »* au respect de la vie privée. La jurisprudence postérieure est venue confirmer cet arrêt (Cass. Soc. 14 mars 2000). C'est aussi ce qui ressort de la Loi « Informatique et Liberté » en son premier article du 6 janvier 1978.

Dans un arrêt du 31 janvier 2001, la chambre sociale a décidé que *« s'il est interdit à l'employeur de se servir de moyens de preuve obtenus à l'aide de procédés de surveillance qui n'auraient pas été portés à la connaissance des salariés, l'employeur est libre de mettre en place des procédés de surveillance dans des locaux dans lesquels les salariés ne travaillent pas »* (en l'espèce des entrepôts). De nombreux juristes estiment que cet arrêt pourrait être applicable à un salarié visitant des sites ou des pages auxquels il n'aurait pas dû avoir normalement accès. C'est dans ce sens que la CNIL, dans son rapport 2000, estime que *« s'ouvre l'ère du « contremaître virtuel » pouvant tout exploiter sans que le salarié en ait forcément conscience, et permettant le cas échéant d'établir, au-delà des légitimes contrôles de sécurité et de productivité des salariés, le profil professionnel, intellectuel ou psychologique du salarié virtuel ».*

Cependant la loi impose le respect de certaines procédures avant tout contrôle par l'employeur. Ainsi, le comité d'entreprise doit être informé et consulté préalablement à la décision de mise en œuvre de l'entreprise, sur les moyens ou techniques permettant un contrôle d'activités des

[117] www.cnil.fr
[118] Cf. citation Ph. Waquet, Droit social décembre 2000 p.1051

salariés. Aussi, en vertu de l'article L 121-8, *« aucune information concernant personnellement un salarié ne peut être collectée par un dispositif qui n'a pas été préalablement porté à sa connaissance ».* Un oubli d'information préalable rendrait inopposable au salarié l'éventuel contrôle effectué.

Il faut noter que la chambre criminelle se fonde sur une autre logique.
Pour cette dernière, *« aucune disposition légale ne permet au juge répressif d'écarter des moyens de preuve produits par les parties au seul motif qu'ils auraient été obtenus de façon illicite ou déloyale »*[119].

Concernant la production de documents émanant de l'entreprise, la chambre sociale estime qu'un salarié peut produire en justice *« des documents contenant des informations dont les membres du personnel pourraient avoir normalement connaissance »*[120], donc par exemple l'essentiel des pages intranet accessibles sans code d'accès.
Pour la chambre criminelle, il peut s'agir par exemple d'un vol[121].

Au sujet des e-mails ou des dossiers personnels figurant dans le disque dur (arrêt du 4 avril 2001 déjà cité), et même si elle le souhaite vivement, l'entreprise peut-elle raisonnablement prétendre que la vie professionnelle soit exclusive de toute vie personnelle ?

Qu'en est-il de e-mails adressés à un collègue mêlant informations professionnelles et personnelles ?

c- La confusion entre vie privée et vie professionnelle : le secret des correspondances

Les questions juridiques liées au courrier électronique au bureau sont complexes et les points de vue sont parfois divergents. Du coté du salarié, les NTIC permettent de conserver toutes les traces laissées par la personne connectée. Ainsi, un message électronique que le salarié avait cru avoir

[119] Cass. Crim. 6 avril 1994
[120] Cass. .Soc. 2 décembre 1998
[121] Cass. Soc., 16 mars 1999

supprimé peut avoir été sauvegardé sur un serveur de messagerie ou sur un support magnétique de sauvegarde. Mais il faut relativiser ses pratiques. Nous sommes quand même loin du modèle anglais ou américain où les statistiques indiquent que plus des deux tiers des entreprises contrôleraient le courrier électronique de leurs salariés (en utilisant des logiciels comme celui du nom de « little brother »).

Un mail intercepté par l'employeur est-il considéré comme une violation du secret des correspondances ?

La 17^{e} chambre du tribunal correctionnel de Paris s'est prononcée à ce sujet le 2 novembre 2000 à propos d'un directeur de laboratoire ayant pris connaissance de la messagerie électronique puis du disque dur d'un thésard en informatique : la révélation du contenu et le fait qu'à lui seul, il était l'auteur de la moitié du courrier électronique d'un laboratoire de 70 personnes à conduit à une fin de thèse anticipée. Le tribunal a décidé que l'envoi de messages électroniques constitue une correspondance privée, il y avait donc violation de l'article premier de la loi du 10 juillet 1991 sur le secret des correspondances et de l'article 8 de la CEDH. En l'espèce, le directeur du laboratoire a été condamné à 10000F soit 1524 Euros d'amende et il en a été de même pour l'ingénieur système.

Les e-mails commencent à épaissir les dossiers contentieux et certains employeurs en viennent à inviter leur encadrement à systématiquement imprimer les mails officiels avant de les envoyer. Ainsi des e-mails de félicitations, rapports hiérarchiques flatteurs pourront ensuite invalider un licenciement pour insuffisance professionnelle par exemple, ou encore les heures nocturnes d'envoie constatant des journées de travail excessives, et seront produis par écrit en justice.

Il est nécessaire de citer également l'arrêt de la Cour de cassation du 2 octobre 2001, l'arrêt NIKON. En l'espèce, Onof, chef du département topographie de la société Nikon, est soupçonné d'activités parallèles sur le temps de travail. Il accumule les plaintes des clients et les relations sont particulièrement tendues avec la hiérarchie, et il aurait pu être licencier à cause de ces éléments. Mais l'employeur va ouvrir le disque dur du collaborateur et prend connaissance de deux fichiers, l'un intitulé « personnel » et l'autre intitulé « fax ». En lisant le contenu de ces

fichiers, il y trouve la confirmation de ses soupçons à savoir que M. Onof exerce bien une activité parallèle ce qui lui vaudra un licenciement pour faute grave. La Cour de cassation casse la décision de la Cour d'appel qui justifiait le licenciement pour faute grave en se fondant sur le contenu des e-mails.
Selon la Cour de cassation : *« même au temps et au lieu de travail, le salarié a droit au respect de l'intimité de sa vie privée, qui inclut en partie le secret des correspondances […] l'employeur ne peut dès lors, sans porter atteinte à cette liberté fondamentale, prendre connaissance des messages personnels émis par le salarié ou 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 ».*

Pour les juges, le secret des correspondances ne peut être violé même si l'employeur interdit toute utilisation non professionnelle de l'ordinateur mis à disposition. Cet arrêt est dans la continuité de la tendance jurisprudentielle de la Cour de cassation quant à la protection des libertés fondamentales. Ce qui est dans la lignée de l'article 7 de la Charte adoptée à Nice en décembre 2000 : *« Toute personne à droit au respect de sa vie privée et familiale, de son domicile et de ses communications ».*

En résumé, l'employeur n'a pas le droit de prendre connaissance du contenu des messages électroniques personnels, ni des appels téléphoniques des employés quand bien même il aurait interdit l'usage du matériel professionnel par le salarié à des fins personnelles. Le respect de la vie privée s'impose, même au bureau. Les e-mails sont protégés par le secret des correspondances au même titre que les courriers sur support en papier, sous plis etc. L'employeur ne peut prendre connaissance de ses messages personnels sans violer le secret des correspondances. Le système britannique soutient le contraire depuis les attentats du 11 septembre. Le RIPA autorise un employeur à intercepter et lire un e-mail d'un salarié sans son consentement et donc à son insu. Jusqu'alors, la législation britannique n'autorisait les interceptions que dans les affaires criminelles et dans des affaires mettant en cause la sûreté de l'Etat.

La jurisprudence fort protectrice de la vie privée du travailleur fait poser une autre question : la Cour de cassation ne semble-t-elle pas cautionner indirectement l'usage de la 'connexion professionnelle' par le salarié à des fins personnelles sous le couvert de l'article 9 du Code civil ? On peut remarquer que la Cour n'a pas sanctionné l'abus du salarié. Cette position mérite une explication. Peut-on l'expliquer par le fait que la vie privée ait un coût nettement plus élevé qu'une connexion Internet ?

Ce point de vue idyllique ne fait cependant pas l'unanimité. En se fondant sur quelques décisions des cours américaines, la doctrine canadienne a répondu différemment à ces questions : les employeurs peuvent surveiller dans toute circonstance qui leur semble appropriée. Ces réponses semblent fondées sur deux prémisses empruntées de la jurisprudence américaine sur le sujet. Premièrement, les salariés ne peuvent prétendre à la protection de leur vie privée lorsqu'ils se servent du courrier électronique et de l'Internet de la compagnie. Deuxièmement, l'employeur étant propriétaire de ces outils, il peut surveiller leur utilisation ad nutum, autrement dit, comme bon lui semble. Toutefois, il serait imprudent de présumer que les tribunaux canadiens suivront la jurisprudence américaine à ce sujet. Il faut prendre en considération des divergences importantes entre les législations américaine et canadienne applicables en la matière.

On peut d'ailleurs se demander si le numérique réalise une fusion entre la vie professionnelle et la vie privée. C'est bien cette ambiguïté que la Cour de cassation a évitée.
Rappelons, au passage, qu'un e-mail peut engager son auteur tout comme l'entreprise en cas de contenu illégal : l'entreprise Ikea s'est retrouvée ainsi devant le Tribunal correctionnel de Versailles début février 2001 car un cadre du service recrutement avait envoyé un e-mail par Intranet à seize cadres de l'entreprise indiquant s'agissant de l'embauche de distributeurs de catalogues : *« pour ce type de travail, ne pas recruter des personnes de couleur car, c'est malheureux à dire mais on leur ouvre moins facilement la porte, et il s'agit d'avancer vite »*. Bien qu'il s'agisse a priori d'Intranet et d'une correspondance privée, la Cour a retenu cet e-mail à titre de preuve et une peine de 30 000F d'amende pour discrimination raciale à été prononcée par jugement du 2 avril 2001.

En la conjoncture actuelle, les e-mails peuvent fournir un motif réel et sérieux de licenciement si leur contenu est injurieux, diffamatoire ou s'ils portent atteinte à la vie d'autrui.

c- La sauvegarde de la vie privée, du lien de subordination et du secret professionnel

Plusieurs catégories de travailleurs partagent le secret professionnel dans le cadre d'un contrat de travail. La plupart des professions libérales relèvent du régime salarié. Médecins, experts-comptables, juristes et leurs personnels sont moins souvent associés et plus souvent salariés dans le contexte économique actuel. Ainsi, le régime salarié de l'avocat en a fait une catégorie à part. Il est à la fois indépendant et subordonné. C'est une loi du 31 décembre 1990 qui a introduit le salariat de l'avocat. Le secret professionnel dans une telle situation prend une dimension 'sociale'. Il passe du 'cadre personnel' de l'avocat seul à un contexte social des avocats en équipe, au niveau supérieur du cabinet, sans pour autant changer de teneur.

S'il est vrai que les NTIC et notamment le télétravail ont permis une plus grande autonomie des travailleurs, il faut remarquer que la subordination, au sens juridique, reste la même : les parties sont toujours liées par un contrat de travail, et le salarié doit rendre compte du travail effectué à un supérieur hiérarchique.

Car même si le supérieur hiérarchique n'est plus physiquement présent à chaque instant, il peut toujours contrôler le télétravailleur, et ce à condition de respecter les procédures d'information posées par le Code du travail. En effet, le juge est très attentif à la loyauté qui doit présider les rapports entre les parties au contrat, et au respect des libertés individuelles et collectives.
Avec la cybersurveillance, on est passé de la traque du salarié à la transparence dans l'exécution du contrat de travail.

De plus, les nouvelles technologies et le recours au télétravail pourraient, dans les années à venir, connaître un second souffle pour au moins deux raisons :

- raison conjoncturelle : pour la période 2001-2003, l'amendement « Messier » consent de très alléchantes exonérations fiscales et sociales aux entreprises donnant un matériel informatique à leurs salariés dans le cadre d'un accord collectif. Il faut avouer que ce don permet de lutter contre « l'illettrisme technologique » dans des entreprises où l'activité économique dépend de l'essor des NTIC. Ceci n'est pas vu d'un très bon œil par les syndicats qui considèrent qu'il risque d'y avoir empiètement de la vie professionnelle sur la sphère privée.

- raison structurelle : avec les possibilité quasi infinies de communication à distance désormais offertes par le réseau Intranet et surtout Internent, le télétravail semble réunir les conditions essentielles de son explosion.

Les NTIC relancent donc un vieux débat, comme le remarquait la CNIL dans son rapport 2000 : *«Elles posent de façon nouvelle des questions qui avaient été réglées dans un contexte ancien. »*
Pour la Haute juridiction, c'est le secret des correspondances et le respect de l'intimité de la vie privée qui priment. Cette position vaut également pour les e-mails, et téléphone au bureau.
En revanche, la vie privée n'est protégée que dans la cybersurveillance limitée à l'entreprise, en l'occurrence sur le lieu de travail. La cybersurveillance administrative ou judiciaire ne connaît pas cette limite.

Enfin, au sein d'une entreprise comme un cabinet d'avocats où le secret est partagé, la cybersurveillance se réduit normalement un contrôle et ne constitue en rien une menace pour le secret professionnel. Notons tout de même que dans cette hypothèse le respect à la vie privée et à l'intimité subsiste.

La CNIL, dans sa recherche d'un équilibre entre l'intérêt à surveiller et la vie privée se heurte souvent à des législations antagonistes à sa mission.

3- <u>La CNIL et la cybersurveillance</u> : la recherche d'un équilibre entre l'intérêt à surveiller et la protection de vie privée

La CNIL joue à la fois un rôle de conciliation et de régulation. Ce qui l'amène à rechercher de l'équilibre dans la cybersurveillance (a). Cependant, force est de constater sa mise à l'écart dans la cybersurveillance 'policière' (b).

a- La recherche de l'équilibre dans la cybersurveillance par la CNIL

Comment accorder vie professionnelle et vie privée au sein de l'entreprise et quels sont les actes de contrôles que la CNIL considère comme admissibles dans le cadre de la cybersurveillance des salariés dans leurs usages d'une messagerie ?

Les trois actes de contrôle admis sont, d'une part, le contrôle du volume des messages échangés, d'autre part, le contrôle de la taille des messages échangés, et enfin, le contrôle du format des pièces jointes. A aucun moment, la CNIL ne considère comme acceptable le fait d'intercepter et de prendre connaissance du contenu des messages.

En revanche, sur autorisation et sous contrôle judiciaire, l'ouverture des messages pourrait être admise.

La CNIL a présenté le 11 février 2002 dernier son second rapport sur la cybersurveillance sur les lieux de travail. Ce rapport tient compte des contributions reçues après la diffusion de son premier rapport présenté en mars 2001. Bâti autour de six grands thèmes, ce rapport a pour but de proposer des instructions, des indices de réflexion permettant de générer un équilibre entre l'intimité de la vie privée des salariés au travail et le besoin de sécurité des employeurs.

- *« Le contrôle des connexions à Internet »*

La CNIL suggère aux employeurs de fixer les conditions d'usage d'Internet dans l'entreprise en informant leurs salariés sur les procédures de contrôle mises en place : dispositifs de filtrage de sites non autorisés, prescriptions légitimes dictées par la sécurité de l'entreprise (interdiction de

téléchargement, d'utilisation de « chat », d'accès à une boîte personnelle, etc.) et contrôle à posteriori des données de connexion, celui-ci étant conseillé de manière globale et non individualisée, et devant faire l'objet d'une consultation du comité d'entreprise. Pour ce qui concerne les employés, la CNIL leur suggère un « usage raisonnable, non susceptible d'amoindrir les conditions d'accès professionnel au réseau ».

- *« Le contrôle de l'usage de la messagerie »*

La Commission reconnaît l'usage raisonnable de la messagerie pour envoyer ou recevoir un message personnel comme habituellement autorisé dans le cadre de l'exécution d'un contrat de travail. L'emploi d'outils de contrôle ou de sauvegarde mis en place pour des raisons d'exigence de sécurité, de prévention ou de contrôle doit être porté à la connaissance des salariés ainsi que la durée de conservation du message « sauvegardé ». Les modalités de contrôle là encore doivent être soumises aux instances représentatives, puis faire l'objet d'une communication auprès des salariés.

- *« Les fichiers de journalisation »*

Ces fichiers permettent d'identifier et d'enregistrer toutes les connexions ou tentatives de connexions à un système automatisé d'informations. Ils ont pour finalité de garantir une utilisation normale des ressources du système et non le contrôle des utilisateurs. La CNIL préconise leur mise en place assortie d'une communication auprès des utilisateurs.

- *« Le rôle des administrateurs de réseaux »*

Par leurs fonctions, ils sont conduits à avoir accès à l'ensemble des informations relatives aux utilisateurs, mais tenus au secret professionnel ils ne doivent en aucun cas divulguer ces informations ni être contraints hiérarchiquement de le faire.

Ce rappel de la soumission des administrateurs de réseaux au secret professionnel est d'une importance capitale pour notre analyse. Car, si la cybersurveillance implique forcément ou alors, quasiment, une atteinte à la vie privée ou à la confidentialité des données nominatives, la soumission à la confidentialité de la cybersurveillance elle même semble être une garantie nécessaire à la sauvegarde du secret.

- *« Les instances représentatives du personnel »*

La CNIL conseille aux entreprises et aux administrations de négocier les conditions dans lesquelles la messagerie de l'entreprise peut être utilisée par les instances représentatives du personnel ou pour l'exercice d'un mandat syndical. Modalités d'utilisation et mesures de confidentialité devant faire l'objet de beaucoup d'attention.

Enfin, la CNIL préconise à l'ensemble des entreprises l'établissement d'un bilan annuel *«informatique et libertés »* à l'occasion du bilan social de l'entreprise et la désignation d'un délégué à la protection des données.

L'intérêt de l'intervention de la CNIL dans les rapports sociaux est également lié au fait qu'elle n'est pas une machine essentiellement répressive. Elle joue un rôle de conciliation et de régulation dans les contentieux relatifs aux données. Ainsi, plusieurs situations anormales ont-elles été régularisées. Qu'en est-il de son rôle lors que la cybersurveillance devient policière ?

b- La mise à l'écart de la CNIL dans la cybersurveillance 'policière'

Le fichage 'policier' s'est intensifié depuis les attentats et la législation semble manifestement, et de plus en plus, écarter la CNIL du contrôle des fichiers policiers.
Cela explique peut-être la défiance des sénateurs socialistes à l'égard du projet de loi dite *« loi d'orientation et de programmation pour la sécurité intérieure »* (LOPSI) qui vient renforcer de la surveillance des réseaux. Les sénateurs socialistes exigeaient un encadrement plus strict des procédures censées permettre à la police d'accéder à distance aux données conservées par les opérateurs de télécommunication et par les fournisseurs d'accès à internet. Ils demandaient que des discussions soient engagées avec ces prestataires techniques et que la CNIL soit consultée sur le sujet. Adopté en première lecture par l'Assemblée nationale, le 17 juillet 2002, ce projet de loi a été adopté par le Sénat, sans modification, le 31 juillet 2002. L'effet ne s'est pas fait attendre : le Conseil constitutionnel a été saisi en application de l'article 61, alinéa 2, de la Constitution, par plus de soixante députés, le 5 août 2002.

La CNIL est la garante de la protection des données personnelles informatisées. Sa dénomination et la loi de 1978 qui l'a instituée sont suffisamment claires là-dessus. La doctrine, la jurisprudence et le législateur semblent unanimes dans la reconnaissance de cette institution. Ces mots de P. LECLERCQ, Conseiller à la Cour de cassation et membre de la CNIL méritent un moment d'attention : *« Le législateur de 1978 a fait preuve de vigilance particulière à l'égard de l'Etat et des administrations publiques ; il s'agissait fondamentalement de reconnaître à un moment où l'Etat s'informatisait, et où apparaissait menaçant le renforcement d'un Etat-Leviathan informatisé, des garanties nouvelles aux citoyens ou aux administrés. La loi du 6 janvier 1978 porte incontestablement témoignage de cette méfiance d'origine, accordant à la CNIL des pouvoirs considérables pour le contrôle préalable et permanent d'informatisation du secteur public »*[122]. A la lecture de ce passage, on peut penser que la CNIL garantit l'effectivité des libertés liées aux données informatisées. Dès lors, la mise à l'écart d'une telle institution du traitement des données qui relèvent de la vie privée peut inquiéter, surtout lorsque c'est la police qui intervient.
Consciente de ses limites, face au risque d'atteinte aux droits et libertés individuelles, la CNIL semble désormais privilégier le rôle d'information à celui de la réglementation.

En outre, la pratique de la cybersurveillance systématique ou quasi-systématique constitue en effet une remise en cause ou bien un contournement de la présomption d'innocence qui reste pourtant un droit fondamental.

4- <u>La présomption d'innocence : un droit fondamental oublié</u> ?

a- La notion de présomption d'innocence

«*Toute personne suspectée ou poursuivie est présumée innocente tant que sa culpabilité n'a pas été établie. Les atteintes à sa présomption d'innocence sont prévenues, réparées et réprimées dans les conditions prévues par la loi »*[123] : voilà qui donne à cette analyse tout son suc.

---

[122] LECLERCQ P., La CNIL, garante de la finalité, de la loyauté et de la sécurité des données personnelles, in Les libertés individuelles à l'épreuve des NTIC (déjà cité), éd. PUL, 2001, p.111

[123] LOI no 2000-516 du 15 juin 2000 renforçant la protection de la présomption d'innocence et les droits des victimes (article 1e , alinéa 3), J.O. Numéro 138 du 16 Juin 2000 page 9038

La présomption d'innocence aura été des mots les plus prononcés pour ne pas dires célèbres du débat judiciaire. La présomption d'innocence a fait du chemin avant la réforme de la procédure pénale qui lui a donné encore plus de notoriété. Héraclite, le philosophe grec mort en 480 avant Jésus-Christ, écrivait déjà à son époque : *« J'appelle la présomption un mal sacré et la vue, un mensonge »*. Ce qui implique que ce qui est 'supposé' doit s'accompagner d'un certain nombre d'observations particulières pour fonder une vérité, un jugement.

Ce terme de « présomption » couve-t-elle une réalité particulière pour un juriste ?

Du latin 'praesumptio' qui signifie conjecture et de 'praesumere' signifiant prendre d'avance, il renvoie imparablement à l'idée d'un jugement fondé non pas sur des preuves, mais sur des indices et sur des apparences. Cette supposition que l'on tient pour vraie dans la pratique y demeure jusqu'à preuve du contraire. Or, dans le doute, la présomption doit être en faveur de l'accusé : *« le doute profite à l'accusé »*. Il y a, d'ailleurs, une indéniable corrélation entre ce principe et celui de la légalité des délits et des peines. Mais que l'on parle de *« présomptions légales »* ou de *« présomption de fait »*, elles demeurent des déductions tirées à partir de faits connus pour établir la vraisemblance d'un fait inconnu. Les présomptions appartiennent habituellement au nombre des modes de preuve.

Encore à ce niveau une distinction est possible : il existe des présomptions simples et des présomptions irréfragables. Ainsi, sont des présomptions *«irréfragables ou absolues»*, celles qui ne souffrent pas de preuve contraire. Les présomptions *«simples ou relatives»* celles dont les preuves contraires sont légalement recevables.

En résumé, la présomption d'innocence est ce principe selon lequel un individu sur qui pèsent des soupçons de demeure innocent, jusqu'à ce que le jugement de sa culpabilité ou de son innocence soit rendu. L'innocence est la règle et la culpabilité, l'exception. N'est-ce pas porter atteinte à la dignité et à l'honorabilité d'une personne que de la juger coupable sans preuve ? Cela pourrait expliquer que la notion 'd'inculpation', qui porte en lui la culpabilité, cède désormais la place à celle de 'suspicion et de poursuite' dans le nouveau langage de procédure pénale.

Posé par l'article 9 de la Déclaration des droits de l'homme et du citoyen du 26 août 1789, le principe de la présomption d'innocence est un principe à valeur constitutionnelle. Un examen

de constitutionnalité de la loi portant diverses mesures relatives à la sécurité routière et aux infractions sur les agents des exploitants de réseau de transport public de voyageurs a récemment été pour le Conseil constitutionnel l'occasion de le rappeler[124].

De ce fait, on peut, d'ores et déjà, se demander si la cybersurveillance qui n'a qu'une valeur législative peut méconnaître la présomption d'innocence sans être anticonstitutionnelle. Cette question posée, on peut se rappeler le refrain de cet article *«Le piège sécuritaire. A qui profite la surveillance ?»* (signé les Virtualistes) publié le vendredi 19 octobre 2001 sur le site de l'association LSI Jolie : *«Nous sommes tous des terroristes potentiels».* Publié 4 jours après la LSQ, cet article était une réaction contre la cybersurveillance telle que prévue par celle-ci. D'ailleurs, tout slogan qu'ils sont devenus, ces mots souvent repris dans cette lutte. L'article du 19 octobre dénonçait non seulement la violation systématique de la vie privée mais aussi le caractère suspicieux des mesures de cybersurveillance à l'égard de tous. Sans le moindre indice de culpabilité d'actes terroristes ou de blanchiment d'argent (ou de complicité avec les réseaux terroristes, de blanchiment d'argent etc.), ces mesures exigent, a priori, la *«transparence de toutes nos communications, téléphoniques, électroniques et pourquoi pas postales. Portes dérobées dans nos logiciels et ordinateurs. Anonymat interdit. Cryptage toléré si décryptage accepté. Si non, procédure secret-défense, échappant aux magistrats et à tout recours pour les victimes»*[125].

Quelle est donc l'incidence de la cybersurveillance sur l'effectivité de la présomption d'innocence?

b- La cybersurveillance : de la violation à l'oubli de la présomption d'innocence

L'article 9-1 du Code civil est sans ambiguïté : *« Chacun a droit au respect de la présomption d'innocence »*. Dans un arrêt du 6 mars 1996, la Cour de cassation précisait que *«l'atteinte à la présomption d'innocence visée à l'article 9-1 consiste à présenter publiquement comme*

[124] Décision n° 99-411 DC, 16 juin 1999, consultable sous http://www.conseil-constitutionnel.fr
[125] http://www.lsijolie.net/article.php3?id_article=69

coupable, avant condamnation, une personne poursuivie pénalement »[126]. En principe, la présomption d'innocence ne s'applique ne s'applique qu'aux affaires pénales. Autrement dit la présomption pénale devient nécessaire lorsqu'une infraction est commise. Si la présomption d'innocence sous-entend que toute personne qui n'est pas condamnée ne soit pas présentée comme coupable, elle signifie, a fortiori, que toute personne qui n'est pas soupçonnée ou mise en examen se sente complètement libre et tranquille.

Cela étant, notons que la cybersurveillance systématique et générale du même type que celle prévue par LSQ répond à deux exigences : la nécessité de garantir la sécurité des personnes et des biens ou de garantir l'ordre public en générale ; il y a également lieu de rechercher les complices éventuels des attentats du 11 septembre 2001 ou les membres du réseau Al-Qaëda de Ben LADEN qui sont recherchés par la Justice. Mais, comment garantir la sécurité si les terroristes potentiels sont en liberté et sans aucune surveillance ? Cette question semble trouver réponse que dans un dilemme : garantir l'ordre public en violant certains droits fondamentaux des citoyens (la vie privée, la présomption d'innocence…) ou alors, prendre le risque de ne pas prendre des mesures préventives à la hauteur des menaces. Or, lorsque la loi soumet des honnêtes gens à des mesures qui sont par définition destinées aux criminels, aux criminels potentiels ou alors à leurs complices, on peut bien se poser la question de savoir si la présomption d'innocence existe encore.

En effet, plusieurs parmi des personnes que nous avons interrogées ont le sentiment d'être *«traquées comme de vulgaires malfaiteurs »* (un avocat parisien) ; un expert-comptable parisien *«on a touché le fond cette fois-ci »*; d'autres personnes se demandent encore pourquoi elles sont traitées comme de terroristes ; et une partie de ces personnes reste complètement indifférente.

Le 29 mai, le parlement Européen a voté la Directive relative à la protection de la vie privée dans le secteur des communications électroniques. Par 340 voix pour et 150 contre, les parlementaires européens ont ouvert la voie à une cybersurveillance 'générale et exploratoire' des données de connexion. Désormais, les états peuvent surveiller l'ensemble des activités électroniques, du téléphone portable aux sites Web visités, en passant par la lecture de tous les e-mails. Ce vote fit

[126] Civ. 1re 6 mars 1996 : Bull, civ. I, n° 123; d. 1997. Somm. 73, obs. Dupeux

l'objet de vives contestations et un député Européen, l'écologiste allemande Ilka SCHROEDER, s'écria : *« C'est encore plus fort que la Stasi !».*

Soulever à ce niveau de notre étude la question de la validité des mesures de la cybersurveillance dans la lutte contre le terrorisme et le trafic nous permettra de mieux cerner l'ensemble des réformes législatives qui continuent de marquer l'après 11 septembre.

Titre III / La validité des mesures de la cybersurveillance dans la lutte contre le terrorisme, le trafic et le blanchiment

Les novelles technologies de l'information et de la communication (NTIC) constituent un instrument au service des réseaux de trafic, de blanchiment de fonds et terrorisme, mais elles en sont autant la cible. Une jurisprudence plutôt abondante fait prendre conscience du problème.
La réaction des pouvoirs publics s'est considérablement accentuée depuis les attaques terroristes du 11 septembre 2001. Une série de législations ad hoc favorable à la cybersurveillance se trouve être le moyen de lutte contre les réseaux terroristes. De ces législations de circonstance, on assiste à une crainte : la crainte d'une dérive totalitaire (chap. I). Aussi, face à l'essor du blanchiment d'argent, une problématique émerge : le déclin du secret professionnel (chap. II).
Remarque : la validité est la condition de toute mesure dans un Etat de droit. C'est bien pour cela que les deux chapitres qui suivent soulèveront la question de la validité des mesures de cybersurveillance étudiées.

Chapitre I / La lutte contre les réseaux terroristes : de la législation de circonstance à la crainte d'une dérive totalitaire

Parce que la loi l'a voulu, la lutte contre les réseaux terroristes implique la consécration de la cybersurveillance 'policière'. (1). Du coup, la question va se poser de savoir si la LSQ est une

mesure de police administrative ou une mesure de police judiciaire permanente (2). La cybersurveillance systématique semble réaliser une obligation de violation et une violation légalisée du secret professionnel (3), parce que la cybersurveillance telle que prévue par la LSQ et la LOPSI s'opère au mépris du privilège de confidentialité. (4)

1- <u>La consécration de la cybersurveillance 'policière'</u> : une réforme de circonstance ?

On assiste depuis les attentats du 11 septembre 2001 à la mondialisation de réglementations (cybersurveillance 'policière') particulièrement liberticides. Si l'on n'admet pas que les attentats du 11 septembre 2001 constituent la cause directe des réformes qui ont introduit ou légalisé la cybersurveillance, ils l'ont, à tout le moins, accélérée en tant que mode de prévention. Ainsi, elle se trouve être la réaction législative nationale (a), internationale(c), communautaire (c). Ces réformes de circonstance font poser la question de leur validité axiologique (d).

a- Le 11 septembre ! : La cybersurveillance 'policière' comme réaction nationale

A en croire le dernier rapport de la CNIL et surtout les commentaires de son président Michel GENTOT, *« il n'y a pas d'effet 11 septembre constaté »* dans le secteur d'Internet, dans le cyberespace (Propos tenus à cette occasion dans les médias, notamment dans un article du Monde Interactif daté du 16 juillet 2002, par ce dernier). Ce point de vue n'est pas partagé de tous.

L'*« USA Act »,* sigle d'*« Uniting and Strenghtening America »* que l'on pourrait traduire par *«Unir et renforcer l'Amérique »*, adopté par le Sénat, est des premières mesures par lesquelles, les autorités américaines entendaient renforcer la sécurité et lutter contre le terrorisme. Cette mesure survenait dès le mois d'octobre et devançait de quelques jours une loi intitulée *«PATRIOT Act»*, acronyme de *« Provide Appropriate Tools Required to Intercept and Obstruct Terrorism »* que l'on pourrait traduire par *« Donner les moyens appropriés pour déceler et combattre le terrorisme »* adoptée par la Chambre des représentants. La littérature

même de ces mesures semble assez révélatrice du désarroi qui s'est emparé des Etats-Unis. *« A cela s'ajoute une définition particulièrement extensive du « terrorisme », qui y assimile tout acte de piratage informatique au sens d'une intrusion non autorisée dans un système, serveur ou site Web gouvernemental »*[127].

Il suffit d'accéder frauduleusement à un site Web non autorisé du gouvernement américain pour être inculpé pour acte de terrorisme. Dans cette optique l'élément intentionnel qui caractérise l'infraction pénale semble perdre de son sens. Mais dès lors que le législateur adopte une telle définition du terrorisme, il semble valide, à l'égard de la théorie idéaliste de Kelsen. En effet, si le législateur américain ne semble pas être fidèle au présupposé du terrorisme que la loi définissait jusqu'alors différemment que le piratage, il faut reconnaître que la mesure elle-même répond au paradigme de loi, vu son mode d'élaboration. C'est la validité formelle.

Les autorités publiques sont dotées de nouveaux pouvoirs dans la lutte contre le terrorisme. Lesquels nouveaux pouvoirs permettent désormais une maîtrise de l'information et des réseaux de communication. Les USA pratiquent légalement et sans ambages de la cybersurveillance. Des procédures simplifiées et des droits élargis pour permettre aux agences gouvernementales (CIA, NSA, INS, et autres services secrets civil et militaire) d'échanger leurs informations et de les croiser. Les agences gouvernementales peuvent recueillir proactivement des informations en dehors d'une enquête, sans le signaler aux personnes visées, et les réutiliser éventuellement ultérieurement si une enquête devait viser ces personnes. C'est ce que Me T. VERBIEST appelle *« partage et de collecte proactives d'informations ».*

Ce n'est plus « Echelon » (qui fait mine d'espion) qui exécute ce programme mais Carnivore. Carnivore suit à la trace tous les e-mails et surfs sur Web. On assiste à l'élargissement des écoutes administratives. La loi facilite ces écoutes en autorisant dans certains cas de ne pas

---

127 Thibault Verbiest, *Terrorisme et Internet: vers une dérive sécuritaire*, 25 mars 2002
Consultable sous : http://www.droit-technologie.org/1_2.asp?actu_id= 554

spécifier les numéros des correspondants écoutés. Or, faut-il le clamer fort, la cybersurveillance ainsi définie est nécessairement attentatoire aux libertés individuelles. La licéité d'une mesure n'empêche pas qu'elle porte atteinte aux libertés, au contraire, elle le justifie.

Le même climat de terreur a conduit la Grande-Bretagne a adoptée à la mi-décembre 2001 le RIPA qui permet une cybersurveillance systématique et généralisée. Par exemple, le RIPA permet la soumission des salariés à la cybersurveillance sans limite et sans le respect du droit au respect de la vie privée, fait des salariés des *« usual suspect »* ('suspects habituels', mais à comprendre comme 'suspects éternels'). Le texte est assorti d'une annexe sous forme d'une *«Supplemental Regulatory Impact Assessment : Retention of communications data»* qui se veut une sorte de code de bonne conduite pour les fournisseurs.

Cette mutation dépasse le cadre national. Le droit international et le droit communautaire vont connaître de grandes réformes.

b- Le 11 septembre ! : La mondialisation de la cybersurveillance

A l'instar des Etats-Unis et face à la mondialisation de la menace terroriste, le droit international subit des réformes notables. Le 23 novembre 2001, trente Etats membres du Conseil de l'Europe ont signé à Budapest la Convention sur la cybercriminalité. La Convention énonce notamment que chaque Partie adopte des mesures législatives nécessaires pour veiller à la conservation rapide des données relatives au trafic, quel que soit le nombre et la qualité des fournisseurs de service qui ont participé à la transmission de cette communication.

Le rapport explicatif précise que ces nouvelles mesures ont vocation à assurer l'effectivité des procédures classiques de collecte, comme la perquisition et la saisie en dépit de l'instabilité des NTIC.

La cybersurveillance tend ainsi à être mondialement reconnue comme moyen légal de lutte contre le terrorisme et la cybercriminalité.

c- Le 11 septembre ! : La cybersurveillance dans la législation communautaire

Au plan communautaire, les évènements du 11 septembre 2001 n'ont fait qu'accélérer un mécanisme déjà en route depuis le traité de Maastricht du 07 février 1992. En effet, à cette date, avait été décidée la création d'une organisation européenne de mise en application des lois, afin d'améliorer l'efficacité des services compétents des Etats membres et leur coopération pour la prévention et la lutte contre le terrorisme, le trafic de stupéfiant.[128] La concrétisation a eu lieu le 1er juillet 1999, lors du démarrage effectif de l'ensemble des activités de cette entité européenne, appelée Europol, soit neuf mois après l'entrée en vigueur de la convention ratifiée par l'ensemble des Etats membres. Sa mission consiste à faciliter l'échange de données à caractère personnel ou non, que celles-ci soient communiquées par les services de renseignements nationaux ou des particuliers.

En outre, l'article 6 du projet du projet de directive qui remplacera la directive 97/66 du 15 décembre 1997 relative aux télécommunications énonce le principe d'effacement des données. Ainsi, les données personnelles stockées par un fournisseur de réseau Internet ou de télécommunications doivent être effacées ou rendues anonymes dès l'achèvement de la transmission. Le 27 novembre 2001, la Commission avait organisé une audition publique consacrée aux données de connexion dans le cadre du European Forum on Cybercrime.

Cependant, au lendemain des attentats, *« la formule ne fait plus recette, même pas dans l'opinion publique légitimement apeurée et assoiffée de sécurité »*[129]. Le 29 mai 2002, le parlement Européen a voté la Directive relative à la protection de la vie privée dans le secteur des communications électroniques. Elle est vivement critiquée, mais n'en demeure pas moins valide au regard du droit communautaire.

[128] Feuille d'information de l'Office européen de police (juillet 1999)
[129] Thibault Verbiest, *Terrorisme et Internet: vers une dérive sécuritaire*, 25 mars 2002
Consultable sous : http://www.droit-technologie.org/1_2.asp?actu_id= 554

d- Les réformes post-11 septembre -réformes de circonstances- et la question de la validité axiologique

Ces réformes sont-elles des réformes de circonstance ? Il est facile de croire que faute des événements du 11 septembre, ces réformes n'auront pas lieu. Cela dit, il convient de les replacer dans leur contexte. Dans plusieurs cas, elles sont dites limitées dans le temps. Par exemple, en France, la LSQ est prévue pour une durée de deux ans et demi. Or rien ne laisse augurer la fin des réseaux et des idées terroristes dans les mêmes délais. Alors, elles auraient servi à quoi, à narguer ? Réformes de circonstance aussi, parce que c'est le climat de terreur dans lequel elles sont réalisées qui favorise leur acceptabilité. Nous serions tentés de croire que la circonstance fait le caractère de la mesure. La LOPSI semble confirmer notre thèse quant on se souvient du *« climat d'insécurité »* qu'elle est censé éradiquer. 'Réponse du berger à la bergère'? Une norme doit-elle sa validité à son acceptabilité ?

Quand on se réfère à la théorie d'Aulis AARNIO[130], la validité d'une norme dépend de son acceptabilité : c'est la validité axiologique. Cette validité est celle du caractère justifié des normes. C'est le contenu rationnel d'une norme qui lui confère toute son autorité. Pour Aarnio, la validité de la norme dépend de son acceptabilité rationnelle. Dès lors, c'est seulement lorsqu'au nom d'une certaine rationalité une norme est jugée acceptable qu'elle est valide.

A contrario, les normes qui ne sont pas justifiables ne constituent pas de normes valides. On peut se rappeler ici la jurisprudence François MASPERO du Conseil d'Etat[131].
Dans ses conclusions, le Commissaire du gouvernement a estimé qu'il y avait une *« erreur manifeste d'appréciation »* qui est une erreur grossière, parce que les mesures de police n'étaient

[130]Aulis AARNIO, Le Rationnel comme raisonnable. La Justification en droit, LGDJ, 1992

[131] CE Ass., 2 novembre 1973, S.A. Librairie François Maspero, RDP 1973. Arrêt consultable sous http://www.rajf.org/ce/ce02111973.php/ Dans cet arrêt, le Conseil d'Etat décida d'approfondir son contrôle de la légalité des décisions ministérielles prises sur le fondement de l'article 14 de la loi du 29 juillet 1881, en étendant celui-ci à l'erreur manifeste d'appréciation, c'est-à-dire en vérifiant que ces décisions ne sont pas affectées d'une grave erreur d'appréciation consistant en une disproportion manifeste avec les faits qui les ont provoquées. Le Conseil d'Etat indique en effet qu'il appartient au juge administratif « de rechercher si la publication interdite est de nature à causer (aux intérêts généraux qui relèvent de la responsabilité du Ministre) un dommage justifiant l'atteinte portée aux libertés publiques ».

pas justifiées par les circonstances et n'étaient donc pas adéquates. La norme, à la lumière du Contrat social de Rousseau, semble tirer sa validité de l'adhésion collective des citoyens.

Des menaces graves d'atteinte à la sûreté de l'Etat, à la sécurité nationale et plus généralement à l'ordre public semblaient justifier les mesures renforçant la sécurité depuis le 11 septembre 2001. Mais la cybersurveillance généralisée est-elle vraiment nécessaire ? En effet, nous savons que les terroristes peuvent toujours se regrouper et que les transferts de fonds peuvent se faire en espèces par des échanges de mallettes, contournant ainsi les réseaux de télécommunication (comme dans un film de mafia). L'atteinte à la vie privée et aux libertés fondamentales sont-elles forcément le prix de l'ordre public ?

« César Borgia avait été tenu pour cruel. Mais cette sienne cruauté avait rassemblé la Romagne, réduite en paix et fidélité » : Machiavel nous a enseigné que la validité d'une norme se passe de son acceptabilité par les sujets[132]. La norme est une expression de la volonté régalienne et non de la volonté citoyenne[133].
La norme valide, selon Austin, est celle qui est imposée par le commandement du souverain. *« Dura lex, sed lex », « la loi est dure mais c'est la loi ».*
Il faut admettre que derrière la 'validité axiologique' apparaît, à peine voilée, une idée de bon sens et donc de vérité. Faut-il admettre plutôt : *« veritas, non auctoritas facit legem »* (c'est la vérité et non l'autorité qui fait la loi) ?

Quand une loi est bien accueillie par tout le monde, tant mieux. Sinon, tant pis. Elle est valide quand même et par conséquent, applicable, sauf dans le cas où le juge constitutionnel l'aurait déclarée non conforme à la constitution, à la norme fondamentale. Dans le prolongement de notre réflexion, il est possible de se demander si la constitutionnalité ou la conventionalité d'une norme ne constituent pas l'expression de son acceptabilité au regard d'un ordre juridique. Nous dirions « oui », volontiers. A l'évidence, les lois et les traités 'post-11 septembre' qui prévoient la cybersurveillance et que nous étudions présentement ne sont pas invalidés. Il est trop tôt ou, peut-être, trop tard.

[132] Nicolas MACHIAVEL, Le prince, Flammarion, 1992, p.220
[133] A propos, la loi est-elle *« l'expression de la volonté générale »* ou, contraire, l'expression d'une volonté généralisée ?

La loi du 15 octobre 2001 dite Loi Sécurité Quotidienne (LSQ) aura été l'une des lois les plus critiquées de l'histoire de la V^{e} République. Le projet de loi d'orientation et de programmation pour la sécurité intérieure (LOPSI) depuis sa présentation fait couler beaucoup d'encre. La cybersurveillance telle que prévue par cette loi semble être à mi-chemin entre mesure de police administrative et mesure de police judicaire. Vu son caractère, la question se pose de savoir s'il ne s'agit pas plutôt d'une mesure de police judiciaire permanente.

2-La LSQ : une mesure de police administrative ou une mesure de police judiciaire permanente ?

a- La cybersurveillance comme mesure de police : de la LSQ à la LOPSI

Le 15 octobre 2001, l'Assemblée Nationale votait en urgence une loi sur la sécurité quotidienne (LSQ).
Au total, treize amendements, présentés comme renforçant les moyens de lutte contre le terrorisme, ont été approuvés le 24 octobre par la Commission des Lois de l'Assemblée Nationale.
Parmi eux, trois amendements concernant à Internet sont issus directement du projet de loi sur la Société de l'Information (LSI) adopté en Conseil des ministres le 13 juin 2001.

Ces mesures combattant le cyberterrorisme, regroupées dans l'article 6 de la LSQ, reposent essentiellement sur la surveillance des informations échangées sur le réseau et, donnent aux juges les moyens de contrer plus efficacement l'utilisation à des fins criminelles des nouvelles technologies de l'information et de la communication.

La LSQ est limitée dans le temps comme en témoigne le moratoire instauré par le gouvernement : ces dispositions, justifiées par la lutte contre le terrorisme, sont proposées au Parlement pour une période limitée au 31 décembre 2003. A cette date, elles feront l'objet d'un rapport qui permettra

d'en évaluer l'application. Ainsi, en changeant de cadre, de la LSI à la LSQ, ces mesures pérennes à l'origine sont devenues temporaires.

Qu'instaure donc précisément la LSQ ?

Principalement trois choses :

- La conservation des données de connexion d'un internaute par les opérateurs de télécommunications y compris les FAI (voir amendement 9, articles 14 à 16 de la LSI).

- Le droit de déchiffrer des messages cryptés (voir amendement 11, dans les annexes).

- L'obligation de remettre les clefs de chiffrement (c'est à dire celles permettant d'ouvrir les mails interceptés par les autorités administratives) à la justice sur sa demande (voir amendements 10 et 11 dans les annexes)[134].

Si, concernant la conservation des données de connexion par les opérateurs, la loi rappelle que le contenu des messages ou informations doit rester secret, elle ne définit pas pour autant qui sont les opérateurs concernés, quels types de données sont visés, ni le délai de stockage de ces informations par les fournisseurs d'accès. On peut penser que c'est pour donner une marge d'interprétation au juge. Ce qui peut être nécessaire, étant donné que les NTIC sont en mutation permanente. Tout n'est pas encore définitif en la matière.

- Qui sont les opérateurs au regard de la LSQ ?

Faute de précision, il semble que cette dénomination englobe à la fois les opérateurs de téléphonie fixe et mobile, les fournisseurs d'accès à Internet et, sans doute, les prestataires de services télématiques. En fait il faudra attendre les délibérations du Conseil d'Etat pour obtenir une définition plus précise.

[134] Voir n° 3 (La LSQ et l'article 226-13 NCP : obligation de violation et violation légalisée du secret professionnel, infra)

De plus, le texte prévoit que les données soient conservées au maximum un an, mais c'est un décret d'application qui devra en fixer la durée définitive. Il y a eu à cet effet un arbitrage du Premier ministre entre le ministère de l'industrie, qui préconisait une durée de trois mois, et le ministère de la justice, qui lui penchait plutôt pour un an. La CNIL préfère elle trois mois. C'est finalement le délai d'un an qui a été retenu.

Que recouvre le terme « données » au regard de la LSQ ?

Ce sont les données permettant l'identification des personnes utilisatrices des services fournis ainsi que les caractéristiques techniques des communications assurées par ces derniers. L'analyse peut se rapporter au temps de connexion de l'internaute aux sites qu'il a visités lors d'une session, en passant par le nombre de mails qu'il a pu échanger. Il faut dire que l'identification est d'autant plus simple dans le cadre d'une entreprise, lorsqu'il revient à contrôler à partir de poste travail inaccessible aux tiers et dont la connexion est protégée par un mot de passe confidentielle.

A l'exception des données techniques nécessaires aux investigations pénales et données nécessaires à poursuivre en recouvrement des factures des opérateurs, les opérateurs devront effacer ou rendre anonyme toute donnée de communication dès lors que cette communication est achevée.

La violation de ces obligations sera passible, tant pour les personnes physiques que pour les personnes morales, d'une peine d'un an d'emprisonnement, d'une amende de 75 000 euros, et d'une interdiction d'exercer cette activité pendant cinq ans.
Toutefois, la conservation des données ne pourra en aucun cas concerner le contenu des correspondances échangées et restera soumise aux prescriptions de la loi *« informatique et libertés du 6 janvier 1978 ».*

Le déchiffrement des messages cryptés ou la fin officielle de la confidence

- Le second point de la loi touche aux fichiers cryptés circulant sur le Net :

L'amendement 11 ne vise pas les interceptions judiciaires, faute de prévoir un régime forçant les prestataires de cryptologie à fournir les moyens de décryptage.
Le législateur permet donc aux autorités judiciaires, grâce à l'amendement 10, de disposer de moyens supplémentaires dans leurs enquêtes pénales lorsque des fichiers informatiques cryptés, qui auront été saisis, et qui n'auront pu être déchiffrés au moyen des clés de déchiffrement fournis par les tiers certificateurs.
Dans un tel cas, le procureur de la République, le juge d'instruction ou la juridiction de jugement pourra confier à une personne qualifiée le soin de procéder au décryptage de ces fichiers.
Il pourra également être fait appel aux moyens secrets des armées si la peine encourue est au moins égale à deux ans d'emprisonnement.

La loi sur la Sécurité Quotidienne permet donc aux services judiciaires, voire aux services secrets, de déchiffrer les messages. Cette loi ne prévoit aucune contre-expertise. En effet, c'est bien ce qu'expriment les articles suivants:
- Article 230-1: *« le procureur de la République, la juridiction d'instruction ou la juridiction de jugement saisie de l'affaire peut désigner toute personne physique ou morale qualifiée, en vue d'effectuer les opérations techniques permettant d'obtenir la version en clair (...) ainsi que, dans le cas où un moyen de cryptologie a été utilisé, la convention secrète de déchiffrement, si cela apparaît nécessaire ».*

- Article 230-4: *« Les décisions judiciaires prises en application du présent chapitre n'ont pas de caractère juridictionnel et ne sont susceptibles d'aucun recours ».*

De fait, la transmission de messages cryptés par la voie d'Internet s'est révélée la forme privilégiée de communication entre membres de réseaux terroristes. Par conséquent, il n'est plus question de réactions purement nationales mais d'une coopération (policière) transnationale pour

de lutter efficacement contre l'utilisation criminelle de la cryptographie. C'est ce problème qu'a soulevé Isabelle ROUJOU DE BOUBEE (la cryptographie : ses nécessités, ses dérives) et que nous avons abordé supra dans la partie consacrée à la cryptographie. Les réseaux mafieux ont souvent recours au langage codé ou hermétique accessible aux seuls membres de chaque réseau. C'est à ce titre qu'ils se servent, volontiers, des cryptogrammes. Il convient pour contrer efficacement le terrorisme et la mafia que les pouvoirs publics puissent accéder à ce langage en utilisant un 'antidote'. Ce dernier consiste à détenir la clef ou alors contraindre ceux qui la détiennent à la rendre, ou à rendre lisibles les messages cryptés.

La nouvelle législation qui renforce la cybersurveillance donne l'impression que l'article 226-13 NCP est de portée relative. Mais on peut se demander si elle ne cache pas une réalité qui est la légalisation de la violation du secret professionnel.

3- La LSQ et l'article 226-13 NCP : obligation de violation et violation légalisée du secret professionnel

a- L'obligation de remettre les clefs de chiffrement à la justice

L'amendement 11 de la LSQ étend, pour le seul domaine des interceptions administratives, à tous les autres prestataires de moyens de cryptologie (éditeurs, importateurs, A.S.P), et cette fois, sans distinction des moyens libres ou des moyens soumis à l'autorisation, l'obligation de remettre aux agents autorisés par la loi les clés de déchiffrement des données cryptées au moyen des prestations qu'ils ont fournies.

Cette disposition vise également à les obliger à effectuer eux-mêmes ce déchiffrement s'ils y sont requis, sauf à démontrer une impossibilité d'y procéder.
L'autorité judiciaire peut donc toujours obtenir la mise au clair d'informations inintelligibles.
La peine, en cas de refus de déférer à ces demandes, est de deux ans d 'emprisonnement, de 30000 euros d'amende et, une interdiction d'exercer cette profession.

Dès lors que les FAI sont obligés à remettre des données confidentielles qui constituent l'essence même de leur soumission au secret professionnel, le secret n'est pas absolu. Non seulement il n'est pas absolu, mais aussi il ne semble pas reposer sur le privilège de confidentialité.

La remise des données confidentielles initialement sécurisées mises à la disposition de la justice à sa demande n'est-elle pas une voix ouverte à l'atteinte au secret professionnel en général (le secret des professionnels qui utilisent l'Internet) ?

Cette obligation devient rapidement dangereuse quand on s'aperçoit qu'aucune exception n'a été prévue par le texte en ce qui concerne certaines professions soumises au secret professionnel. Ainsi, avocats et médecins seront également dans l'obligation de fournir, à toute réquisition judiciaire, les clés de déchiffrement utilisées dans les relations respectives avec leurs clients ou patients. Le risque d'une violation du secret professionnel est donc fortement présent en raison du flou des dispositions en vigueur.

La cybersurveillance est plus que jamais un moyen de contrôle, un instrument de police. C'est dans cet esprit que Lionel Jospin affirmait au lendemain des attentats que la lutte contre le terrorisme passe aussi par une surveillance accrue sur le Net.
Reporters sans frontières rappelait que : *« ...concernant la France, l'adoption de la Loi sur la sécurité quotidienne (LSQ) en novembre 2001 ainsi que tout récemment, le 17 juillet 2002, le vote en première lecture à l'Assemblée nationale de la Loi d'orientation et de programmation sur la sécurité intérieure (LOPSI) ne sont que quelques exemples des mesures édictées et des pratiques liberticides mises en œuvre »*[135].

Le projet de loi d'Orientation et de programmation de la sécurité intérieure (LOPSI), présenté le 10 juillet 2002 par le ministre de la Sécurité intérieure et des libertés locales et adopté le 17 juillet suivant en première lecture par l'Assemblée nationale, vient renforcer la cybersurveillance prévue par la LSQ. Elle comporte, entre autres, une proposition de disposition devant faciliter l'accès direct et la consultation « à distance » par les autorités judiciaires des données de connexion conservées notamment par les opérateurs de télécommunications.

[135] http://www.enduring-freedoms.org/article.php3?id_article=345

Ce projet de loi s'inscrit au nombre des mesures tendant à renforcer l'efficacité des investigations policières. Il a vocation à permettre aux officiers de police judiciaire, qui agissent dans le cadre d'une enquête judiciaire, sur autorisation d'un magistrat, de surveiller des fichiers informatiques et de saisir par la voie télématique ou informatique (cyberperquision) à distance, les renseignements nécessaires à la manifestation de la vérité.

Une telle disposition aurait pour résultat de contraindre les Fournisseur d'Accès Internet à ménager un accès direct et en ligne des autorités aux données stockées par ces prestataires permettant, par exemple, l'identification du titulaire d'une adresse IP qui est souvent nécessaire à l'identification de l'auteur d'une infraction perpétrée en ligne. Ce texte aurait l'avantage d'écourter les délais de transmission par les opérateurs des réquisitions des autorités judiciaires.

En effet, *le Rapport sur les orientations de la politique de sécurité intérieure* précise qu'*« un trop grand nombre d'affaires judiciaires est paralysé par l'incapacité des institutions publiques ou privées (...) à répondre dans des délais raisonnables aux réquisitions effectuées par les officiers de police judiciaire à la demande de l'autorité judiciaire »*.

b- La thèse de la police judiciaire permanente

Il serait intéressant que nous puissions mettre en exergue le trait caractéristique de la cybersurveillance prévue par les deux textes que nous venons d'évoquer. Elle a essentiellement vocation à réunir des preuves en vue de faciliter des investigations judiciaires. En l'occurrence, la rétention de données de communications a pour but de constituer moment venu, la preuve d'une infraction. Elle permet également, comme cela a été souligné plus haut, de suivre à la trace l'internaute. Ce qui permet bien évidemment de corroborer les preuves, et emporter l'intime conviction du juge. Or, le fait même d'aménager des preuves en conservant des données, en interceptant des données téléphoniques etc. consiste à livrer l'auteur d'une infraction à la justice.

Ce principe a notamment été rappelé dans les arrêts Consorts Baud du Conseil d'Etat[136] et Noualek[137] du Tribunal des Conflits.

Doit-on recourir à une conception alternative de la police ou plutôt, à la lumière de l'application de la LSQ, donner une définition mixte de la police : mi-administrative et mi-judiciaire ?

La LSQ dès son origine semble être une mesure de police judiciaire permanente qui ne dit pas son nom. En soumettant les internautes à la surveillance électronique généralisée, la LSQ et la LOPSI font naître une présomption de culpabilité. Dans le cas où tout le monde doit être surveillé, la culpabilité ne devient-elle pas un a priori, la règle et l'innocence, l'exception ? Faut-il désormais établir la preuve de l'innocence ?

Critiquant ces mesures, les associations de défense des droits et libertés fondamentaux, de FAI et d'hébergeurs de sites Internet dont Globenet, Ras l'Front, Act Up-Paris, Samzdat.net …, estiment qu'elles réalisent une *« globalisation de la volonté de porter atteinte à la liberté d'expression ».* Le fait de surveiller de façon aussi soutenue et continue les réseaux, à la recherche de cybercriminels serait mieux défini si l'on parlait de mesures de police judiciaire permanentes.

---

[136]C.E. 11 mai 1951, Consorts Baud : *« Considérant que les requérants demandent à l'Etat réparation du préjudice qu'ils ont subi du fait de la mort du sieur Paul Baud, leur fils, époux et père, blessé mortellement au cours d'une opération de police que des inspecteurs de police accomplissaient à Lyon le 31 octobre 1945 en vue d'appréhender des individus signalés comme faisant partie d'une bande de malfaiteurs ; que cette opération relevait de la police judiciaire ; que les litiges relatifs aux dommages que peuvent cause les agents du service public dans de telles circonstances ressortissent aux tribunaux de l'ordre judiciaire ; que dès lors les requérants ne sont pas recevables à contester devant le Conseil d'Etat la décision du ministre de l'intérieur qui a rejeté leurs demandes d'indemnité ».*

[137] T.C. 7 juin 1951, Noualek : *«Considérant que les faits dommageables dont a été victime la dame Noualek sont consécutifs à une opération de police exécutée dans une période anormale, où en application de textes en date des 23 avril et 7 juillet 1941, tous les services de police étaient placés sous l'autorité des préfets "en vue d'assurer le maintien de l'ordre, de prévenir et réprimer les atteintes à la sécurité publique" ; qu'en l'espèce, ladite opération dont l'instruction n'établit pas qu'elle avait pour objet la recherche d'un délit ou d'un crime déterminé, effectuée sur instructions de l'intendant de police, sous la protection de fusils de chasse, en dehors de tout ordre ou intervention de l'autorité judiciaire, ne saurait être regardée comme une "perquisition", mais comme une véritable opération de police administrative, exclusive des règles protectrices du domicile privé des citoyens, ne pouvant être rattachée au fonctionnement de la justice ; qu'ainsi, dans les circonstances où s'est produit l'acte dommageable, survenu au cours de l'exécution d'un service public et non détachable de l'accomplissement de celui-ci, les tribunaux judiciaires ne peuvent se prononcer sur la responsabilité civile de l'Etat qui n'est susceptible d'être mise en cause que devant un tribunal administratif ».*

En revanche, si la cybersurveillance joue un rôle dissuasif sur les auteurs potentiels d'infraction en ligne, si elle constitue un moyen d'alerte pour les pouvoirs publics qui en tirent parti pour déjouer une atteinte à l'ordre public, on peut admettre qu'elle est administrative. Mais ce n'est pas le trait le plus frappant des deux textes en question.
Toutefois, avec un peu de recul, on se demande si la finalité de la répression des infractions ayant déclancher la cybersurveillance en tant que mission de police judiciaire, n'a pas pour finalité d'assurer le maintien de l'ordre public.

Rappelons-nous qu'on a pu parler de Stasi à propos de ces mesures. Les mots suivants méritent qu'on s'y arrêtent un moment : *« La dénonciation des crimes et délits vise à assurer le respect des lois ; et l'on comprend que les fonctionnaires se voient confier une responsabilité plus importante que les simples citoyens dans l'exercice de cette mission. Une société dans laquelle les lois seraient systématiquement bafouées serait non seulement une société anarchique, mais une société où prévaudrait la loi du plus fort. Mais en sens inverse, si l'on voulait traquer et éradiquer toutes les illégalités, on se dirigerait tout droit vers une société policière, voire totalitaire. Une certaine dose d'illégalisme est la rançon de la liberté »*[138].

L'application de la LSQ heurte l'application effective de l'article 226-13 du Nouveau Code pénal. Tout porte à croire que les deux dispositions, loin d'être applicables simultanément, se rejètent 'dos à dos'. De la contradiction, on parvient à un dilemme : il faut choisir.

Dans un rapport publié récemment par l'Assemblée sur sa mise en œuvre de la loi sécurité quotidienne, les membres de la commission se félicitent de la bonne mise en œuvre de cette loi. La conservation des données de connexion, fichier national des empreintes génétiques est les parties de ce rapport qui nous concernent le plus en raison de leur rapport avec le secret professionnel dont elles sont souvent le soubassement.

[138] Laussinotte, Dénoncer et expulser, Plein Droit n° 27, juin 95

Une lecture du *Rapport de la Commission des Lois Constitutionnelles, de la Législation et de l'Administration Générale de la République*, présenté par M. Bruno LE ROUX serait à cet égard d'une grande utilité. Les mesures introduites dans la loi du 15 novembre 2001 à des fins de lutte contre le terrorisme (articles 22 à 33) ont été adoptées pour une durée allant jusqu'au 31 décembre 2003 ; elles feront l'objet d'une évaluation par le Gouvernement.

Compte tenu des conditions et des motifs de leur adoption, il est étonnant qu'aucune instruction générale relative aux modalités de leur mise en œuvre n'ait encore été publiée par les ministères concernés (les ministères de l'intérieur et de la justice); un télégramme et des notes succinctes ne constituent pas des garanties suffisantes.

Certaines dispositions du chapitre V sont privées d'effet en l'absence d'un décret d'application : les articles 29, 30 et 31 sur la conservation des données de connexion à Internet et le déchiffrement des fichiers informatiques, les décrets correspondants faisant actuellement l'objet de réunions interministérielles.

Pour ce qui est de la conservation des données, il conviendra de veiller à la cohérence du régime mis en place par l'article 29 avec celui institué par l'article 62 de la loi de finances rectificative pour 2001.

En effet, alors que le premier prévoit que les opérateurs de télécommunications, et notamment les fournisseurs d'accès à Internet (FAI) mentionnés à l'article 43-7 de la loi du 30 septembre 1986, sont tenus de conserver lesdites données pendant une période maximale d'un an à la demande de l'autorité judiciaire, le second prévoit que les FAI, mais également les « hébergeurs » mentionnés à l'article 43-8, doivent les conserver pendant trois ans, à la demande, notamment, des fonctionnaires du service des douanes.

En outre, l'article 56 étend le champ du fichier national automatisé des empreintes génétiques (FNAEG). Aussi, le FNAEG avait-il été institué en 1998 pour réunir les empreintes génétiques des seuls auteurs de crimes sexuels ; sa mise en place a cependant été retardée à plusieurs reprises et il n'est devenu réellement opérationnel qu'à la fin de l'année dernière.

La loi du 15 novembre 2001 a élargi son périmètre aux meurtres, tortures et actes de barbarie, vols avec violence, actes de terrorisme. Cette extension est encore subordonnée à la parution d'un décret en Conseil d'Etat qui devra faire l'objet d'une consultation de la CNIL. Le rapporteur souhaite que les écarts qui ont pu troubler la mise en oeuvre du FNAEG ne se reproduisent pas, et, partant, que ce nouveau décret soit publié dans les meilleurs délais.

S'il est vrai que la LSQ prévoit un an pour la conservation des données de connexion, il faut remarquer que la loi de finances rectificative en prévoit trois. C'est ainsi qu'une loi 'technique' vient renforcer, quelques mois plus tard, des dispositions déjà liberticides, en rallongeant leur durée.

Ainsi, la levée du secret professionnel qui était exclusivement judiciaire, réservée au cas par cas, devient légale, c'est-à-dire préétablie par la législation. Il faut surtout noter qu'elle devient obligation pénale aussi.

De ce fait, on ne risque plus rien, lorsqu'en violant l'article 226-13 NCP, on respecte la LSQ (et la LOPSI). Enfin, le secret professionnel ne semble plus justifier le refus de participer à la manifestation de la vérité judiciaire.

On peut, par conséquent, se demander si l'on peut encore faire valoir le privilège de confidentialité.

La traque systématique qui résulte des dispositions de la LSQ peut permettre d'expliquer l'ébauche d'une guerre de constitutionnalité autour de cette mesure.

4- <u>La LSQ : la traque systématique et l'ébauche d'une guerre de constitutionnalité</u>

Pour répondre à cette question, prenons trois exemples : l'un national, le STIC (a), l'autre européen, la convention sur l'entraide judiciaire, (b) et un dernier, international, les cookies (c). La guerre de constitutionnalité est le dernier point de cette sous partie que nous allons aborder (d).

a- Le STIC

La catégorie des personnes mises en cause, qui sont enregistrées dans ce fichier, est entendue très largement.
En effet, sont « fichés » dans le STIC, l'auteur de l'infraction, la victime, les témoins, mais aussi *« toute personne ayant eu affaire avec les services de police ».* Toutes ces personnes y sont enregistrées sous la même catégorie qui est celle des personnes mises en cause.
Par ailleurs, en plus de délits et des crimes, le STIC garde en mémoire certaines contraventions (celles de cinquième classe, les plus graves parmi lesquelles figure le racolage ou l'intrusion dans un établissement scolaire). On y consigne l'identité (nom, prénom, date et lieu de naissance, filiation, nationalité), le signalement, la photographie, les faits et la procédure.

Ces données relèvent de la vie privée et doivent par conséquent bénéficier d'une confidentialité comme le prescrit sans ambages l'article 39 de la loi de 1978 informatique et libertés (nous l'avons cité plus haut).

Parmi les treize amendements que le gouvernement a ajouté au projet LSQ, le huitième (aujourd'hui l'article 28) autorise la consultation de fichiers de police judiciaire (comme le STIC) dans les *« enquêtes administratives d'honorabilité »,* enquête dont les candidats à des missions de sécurité ou de défense peuvent faire l'objet.

La directive européenne relative aux données personnelles aurait dû être transposée depuis 1998, mais le projet n'a été déposé qu'en 2001, après la légalisation du STIC.
Ce texte retire à la CNIL toute compétence en matière de *« fichiers de souveraineté »,* c'est-à-dire relatifs à la sûreté de l'Etat, la défense, la sécurité publique ou la répression des infractions.

Daniel Vaillant a déclaré qu'il comptait sur la CNIL pour éviter les abus. Les déclarations et les politiques effectivement mises en œuvre se contredisent. Or, la CNIL n'a plus les moyens légaux de contrôler les fichiers policiers.

De plus, même si la France a été pionnière de la législation sur la protection des données, la CNIL a été écartée de nombreux dossiers sensibles. Par exemple, en 1999, a été adopté l'amendement Brard qui permet l'interconnexion des fichiers fiscaux et sociaux. C'est cette même question qui avait été à l'origine de la loi de 1978. De même, la vidéosurveillance a été retirée de la compétence de la CNIL par le ministre de l'Intérieur de l'époque (Monsieur Pasqua).

b- l'interception des télécommunications

Cette question a été traitée au niveau européen en l'an 2000 par un acte du Conseil, en date du 29 mai, relatif à l'entraide judiciaire en matière pénale entre les Etats membres.
Ce texte prévoit la possibilité d'y recourir pour les besoins d'une enquête. L'entraide judiciaire peut être demandée afin d'intercepter les communications d'une personne lorsque celle-ci se trouve dans l'Etat membre requérant, si celui-ci a besoin de l'aide technique de l'Etat membre requis pour pouvoir intercepter ses communications, ou lorsque la personne se trouve dans l'Etat membre requis.

Les télécommunications utilisant une porte d'accès (*Gateway*) peuvent aussi être interceptées par l'intermédiaire d'un fournisseur de services téléphoniques.
Le seul point sujet à controverse, posé par l'article 20 de la Convention, était celui de l'interception des télécommunications de personnes sur le territoire de l'autre Etat membre sans son assistance technique.
Certains Etats veulent maintenir la possibilité d'effectuer les enquêtes sans aucune restriction dans un autre Etat, au nom de la sécurité nationale, et refusent toute procédure d'autorisation. L'article précité prévoit une procédure d'information avec la possibilité pour l'Etat membre d'exiger que l'interception ne soit pas effectuée ou interrompue, mais seulement par une décision motivée par écrit.

Le Parlement européen avait, dans un avis en date du 31 janvier 2000, considéré qu'il fallait supprimer l'article parce qu'il aboutissait à reconnaître la possibilité de recourir à des interceptions téléphoniques à titre préventif et de les confier aux autorités judiciaires ; autorités qui n'interviennent, par définition, qu'après qu'une infraction ait été commise.

Il est important de souligner qu'aucune définition n'est donnée des "télécommunications" : s'agit-il des télécommunications par câble, par air, par télématique?
Le Parlement avait considéré qu'un tel vague risquait de multiplier les occasions de litige dans une phase ultérieure.

c- Les cookies

Ils s'installent sur les ordinateurs des internautes après leur première connexion sur le réseau. Ils illustrent ce que peut être un traçage des individus. Ils permettent de dresser le profil de l'internaute jusqu'à constituer une intrusion au cœur de sa vie privée (les Etats répressifs ont déjà utilisé les cookies ou des techniques similaires pour la surveillance de leurs éléments "subversifs".)
Par une décision en date du 14 novembre 2001, le Parlement européen a considéré que les cookies font partie de la vie privée et voulait, par conséquent, en limiter l'usage.

Aujourd'hui, des solutions techniques et juridiques existent pour shunter (court-circuiter) ces fichiers mouchards. On peut tout simplement supprimer les fichiers qui les contiennent.
Les cookies sont soumis à la loi *« informatique et libertés de 1978 »*, ce qui permet aux internautes de bénéficier d'un droit d'accès, de rectification (si les informations sont fausses) et d'opposition (pour des raisons légitimes à l'appréciation du juge).

Le dernier recours est la plainte. En effet, l'internaute peut saisir la CNIL pour qu'elle accomplisse sa mission de contrôle, qu'elle délivre ses avertissements ou dénonce au parquet le site illicite.

Toutes ces méthodes se sont révélées inefficaces face aux attaques terroristes du 11 septembre, attaques qui ont eu pour effet de propulser les interventions étatiques. Cependant elles sont porteuses d'un implacable inconvénient qui est l'atteinte au secret professionnel.

d- La guerre de constitutionnalité autour de la LSQ

Plusieurs associations et ONG ont mené depuis son adoption, une guerre sans merci à la LSQ. L'adoption de cette loi a été pour le moins contestée.

Les premières protestations se sont articulées autour de la méthode des « cavaliers législatifs » utilisée par le gouvernement pour faire voter ces mesures.
Cette pratique, qui a pour effet de limiter le jeu du débat législatif, a déjà été condamnée par le Conseil Constitutionnel, notamment dans sa décision du 29 juin 2000, et déclarée inconstitutionnelle.

Cette pratique est d'autant critiquable qu'en l'espèce ces textes portent sur des mesures susceptibles de porter atteinte à la vie privée ou aux libertés individuelles.

Les internautes sont-ils désormais en liberté surveillée ?
C'est la question que l'on peut se poser à la lecture de cette loi.
En effet, à peine votés, les trois amendements relatifs à Internet ont soulevé de très nombreuses critiques de la part de certaines organisations de protection des droits de l'homme et de la vie privée.
Celles-ci ont estimé que ces amendements pouvaient être liberticides et anticonstitutionnels. Or, l'ultime recours pour ces organismes défenseurs de la vie privée est de saisir le Conseil Constitutionnel, et cela ne peut se faire que grâce à la signature de soixante députés.

Ces différents organismes reprochent en particulier à cette loi l'inefficacité pratique des mesures contre sa cible déclarée, le cyberterrorisme, tout en étant à l'égard des citoyens un instrument d'atteintes graves aux libertés individuelles.
C'est précisément ce qu'a fait remarqué Olivier Iteanu, président de l'Internet Society en France : *« les dispositions de cette loi ne nuiront qu'aux particuliers. Le criminel va passer par d'autres réseaux, utiliser d'autres formes de cryptographie. Surtout, rien ne permet d'affirmer que la personne connectée à Internet soit l'abonné identifié par l'opérateur. Un individu peut très bien usurper l'identité de quelqu'un, et cela n'a pas été intégré dans cette loi ».*

Parmi les groupements protecteurs des libertés, I.R.I.S a lancé une pétition afin de convaincre les personnages de l'Etat qui en ont le pouvoir de saisir le Conseil Constitutionnel de l'examen de cette loi.

D'après le président de l'association *« Imaginons un réseau Internet solidaire »*, prendre comme prétexte les événements du 11 septembre pour dire maintenant que ces amendements ont été prévus pour lutter contre le terrorisme, est véritablement indigne d'autant plus que rien ne prouve que les terroristes ont utilisé Internet d'une manière ou d'une autre pour organiser leurs attaques. C'est donc a priori une loi scélérate, c'est à dire qui se propose d'autres buts que ceux affichés publiquement.
Comme les NTIC permettent la traçabilité des activités sur la toile, le gouvernement en profite pour étendre ses pouvoirs au delà des sphères dans lesquelles il est normalement cantonné dans la vie réelle. Ainsi, l'autorité publique semble devenir une autorité sans limite ou presque sans limite.

Néanmoins, l'amendement 10, qui offre la possibilité pour un juge, dans le cadre d'une perquisition ou d'une enquête judiciaire, de demander aux professionnels de la sécurisation de livrer les conventions secrètes de chiffrement, laisse peu de place aux dérives liberticides de la part du premier ministre ou des juges.

Sur ce point, la LSQ est bien moins dangereuse que celle en discussion aux Etats-Unis. Une tentative d'un particulier a toutefois été faite auprès du Conseil d'Etat. Le 2 novembre 2001, Monsieur Tabaka [139] a présenté, à titre individuel, une requête en référé-liberté dans laquelle il demandait à la plus haute juridiction administrative d'enjoindre le Président de la République de déférer la loi au Conseil Constitutionnel et, dénonçait plusieurs dispositions du texte comme inconstitutionnelles et attentatoires aux libertés fondamentales. Le Conseil d'Etat a rejeté ce recours, au motif que la requête ne relevait pas de la juridiction administrative.
La « saisine citoyenne », demandée par plusieurs associations militantes pour les libertés individuelles, est donc loin de pouvoir suppléer à la négligence des parlementaires.

[139] Référé du Conseil d'Etat en date du 7 novembre 2001

Au delà de ces querelles autour de la LSQ, le blanchiment de l'argent est de plus en plus un argument à la cybersurveillance. En quoi les réseaux numériques favorisent-ils le blanchiment d'argent ?

Dans les années 20, le blanchiment de l'argent est une expression qui a été employée pour la première fois aux États-Unis pour définir la mainmise de la mafia sur des laveries automatiques. A l'époque de la prohibition (origine illicite et criminelle), les gangsters américains mirent cette technique au point en investissant leurs revenus illicites dans une chaîne de laveries automatiques, où les ménagères payaient leur lessive en argent liquide. Les revenus étant exclusivement encaissés en monnaie fiduciaire, les chiffres d'affaires de ces entreprises devenaient incontrôlables, et il ne restait plus qu'à ajouter l'argent sale du trafic d'alcool à l'argent propre des blanchisseries (opération de dissimulation) pour en faire des sommes licites par des opérations de transfert. Ceci offre la possibilité d'investir des revenus occultes dans des entreprises légales (acquisition de biens).

De ce fait, à l'époque, on disait plutôt 'blanchissage' au lieu de 'blanchiment'. La notion juridique de blanchiment n'apparaît que dans les années 80, les faits incriminés alors ne relevant que de la fraude fiscale. C'est d'ailleurs grâce à un contrôle fiscal que le célèbre gangster Al Capone a pu être arrêté[140].

Depuis les attentats du 11 septembre dernier, près de 200 millions de dollars ont été gelés à travers les places financières mondiales dans le cadre de la traque de l'argent sale finançant les actions terroristes. Cette traque s'inscrit dans la logique de la lutte entreprise depuis les années 80 contre le blanchiment de l'argent sale. Pourtant, force est de constater que les outils dont disposent les autorités apparaissent faibles face à l'opacité du secret bancaire de certains

[140] Le samedi 17 octobre 1931, après neuf heures de délibérations, Canpone fut déclaré coupable sous quelques uns des chefs d'accusation d'évasion fiscale. Le samedi suivant, le juge Wilkerson le condamna à onze ans de prison, cinquante mille dollars d'amende et à payer 30 000$ en frais de cour. La caution lui fut refusée et il fut transporté à la prison du comté de Cook en attendant son transfert au pénitencier fédéral. Voir également le New York Times du 24 octobre 1931.

paradis bancaires et fiscaux et face à la rapidité et la fluidité des transactions financières développées dans un contexte de mondialisation et de la révolution numérique.

En effet, selon Luciano Violante[141], *«il faut environ 20 minutes pour transférer par voie électronique des fonds d'un pays à l'autre. Il est possible de déplacer ces même fonds 72 fois en 24 heures d'une partie à l'autre de la planète. Mais, il faut des semaines pour se procurer les preuves de chacun de ces mouvements»*. Et face à la lenteur de la coopération internationale judiciaire dénoncée lors de l'appel de Genève, les blanchisseurs ne cessent de développer de nouvelles techniques de plus en plus modernes en recourant aussi bien aux nouvelles technologies de communication qu'à celles des marchés financiers. Ainsi, le blanchiment qui est une opération consistant à donner une existence légale à des fonds dont l'origine est frauduleuse ou illicite, touche-t-elle à sa finalité par l'interaction de l'économie souterraine du crime organisé sur l'économie légale.

De plus, l'ampleur du phénomène est étendue : le chiffre d'affaires généré par la drogue en 1998 était d'environ 500 milliards de dollars et celui des revenus mondiaux annuels des organisations criminelles transnationales (OCT) sont de l'ordre de 1000 milliards de dollars.

Les statistiques montrent que l'argent blanchi par les organisations criminelles organisées représente un minimum de 320 milliards de dollars par an. Selon un observateur, les performances de la criminalité organisée dépassent celles de la plupart des 500 premières firmes mondiales classées par la revue Fortune. Il faut également prendre en considération l'effet de levier de ces sommes, c'est-à-dire leur pouvoir corrupteur sur le reste de l'économie, et leur accumulation.

En effet, ces profits ont été indistinctement réinjectés sous formes d'investissements légaux. On peut, dès lors, considérer que des pans entiers de l'économie mondiale sont soutenus par de l'argent sale. Le crime organisé envahit le marcher assurant le contrôle de grandes sociétés en étendant leur activité à de nombreux secteurs de l'économie légale rémunérateurs. Une

[141] Président de la chambre des députés italienne

concentration du pouvoir économique par la criminalité organisée peut très facilement se transformer en influence politique.

Un tel pouvoir constitue en fin de compte un danger réel pour la prééminence du droit et de la démocratie : ‘les réseaux’, ‘les affaires’…les vocables ne manquent pas face pour désigner ce phénomène qui fait l’objet d’une jurisprudence florissante. Une approche du mécanisme et des techniques du blanchiment s’avère intéressante comme la question des dispositifs juridiques.

Chapitre II / L’essor du blanchiment d’argent et la problématique du déclin du secret professionnel

Autrefois, seules les banques étaient obligées de déclarer les fonds jugés douteux, qui sont déposés par un client. La NRE du 15 mai 2001 ajoute à ces derniers les organismes financiers dont les sommes inscrites sur les livres pourraient paraître douteuses ou provenir du trafic des stupéfiants ou d'activités criminelles organisées[142]. Ainsi, afin de lutter contre le blanchiment d'argent d'origine criminelle, il a été envisagé de soumettre l'avocat à la déclaration de soupçon. Cela a donné lieu à une controverse que nous essayerons de montrer dans les lignes suivantes (1 et 2). Nous analyserons également la portée du secret bancaire face au blanchiment d’argent sale (3). Pour terminer, nous nous pencherons sur une problématique larvée : le double degré de la cybersurveillance (4).

[142] C. mon. Fin., art L 562, loi n°2001-420, 15 mai 2001, JO 16 mai 2001

1- <u>Le blanchiment d'argent</u> : la cause principale de la remise en question du secret professionnel de l'avocat

L'une des manifestations de la remise en cause de la confidentialité des dossiers et par conséquent du secret professionnel de l'avocat est le débat autour de sa soumission à la déclaration de soupçon. Après avoir défini la déclaration de soupçon (a), nous nous poserons la question de savoir si la déclaration de soupçon ne fait plutôt du défenseur un délateur de conjoncture (b). Il convient d'analyser la cybersurveillance dans l'optique de la perquisition (c).

a. Qu'est ce qu'une déclaration de soupçon ?

La loi oblige certains professionnels ayant des soupçons portant sur des sommes inscrites dans leurs livres ou sur des opérations portant sur des sommes ou opérations qui pourraient provenir du trafic de stupéfiants ou encore d'une activité criminelle organisée de les déclarer à TRACFIN[143].

En principe, la déclaration de soupçon doit être faite avant l'exécution des opérations. Cependant, elle peut porter sur des opérations qui ont déjà été exécutées, lorsqu'il a été impossible de surseoir à leur exécution ou quand le soupçon que les sommes pourraient provenir du trafic de stupéfiants ou d'une activité criminelle organisée est apparu postérieurement à la réalisation de l'opération.

[143] TRACFIN, abréviation de Traitement du Renseignement et Action contre les Circuits Financiers Clandestins, est rattaché au Ministère de l'Economie et des Finances. Ce service a pour mission de recueillir les déclarations de soupçon que les organismes financiers, depuis 1990, les compagnies d'assurance, depuis 1993 et les professionnels de l'immobilier, depuis 1998, ont obligation de lui transmettre au sujet des sommes ou opérations qui peuvent paraître provenir du trafic de stupéfiants ou d'autres activités relevant de la criminalité organisée. TRACFIN analyse ces déclarations et les instruit puis les transmet, le cas échéant, aux autorités judiciaires. TRACFIN a le pouvoir de s'opposer pendant 12 heures à la réalisation d'une opération. TRACFIN a été créé par un décret du 9 mai 1990.

La loi n° 2001-420 du 15 mai 2001 relative aux *« Nouvelles Régulations Économiques »* (N.R.E.) impose des déclarations systématiques ou automatiques pour : Toute opération dont l'identité du donneur d'ordre ou du bénéficiaire reste douteuse malgré les diligences effectuées ; les opérations effectuées par les organismes financiers pour compte propre ou pour compte de tiers avec des personnes physiques ou morales, y compris leurs filiales ou établissements, agissant sous forme ou pour le compte de fonds fiduciaires ou de tout autre instrument de gestion d'un patrimoine d'affectation dont l'identité des constituants ou des bénéficiaires n'est pas connue ; les opérations pour compte propre ou pour compte de tiers avec des personnes physiques ou morales, y compris leurs filiales ou établissements, domiciliées, enregistrées ou établies dans un pays figurant sur la liste GAFI[144].

Sont obligés de faire des déclarations de soupçon, les établissements de crédit, les changeurs manuels, les compagnies d'assurance, les courtiers d'assurances et de réassurance, les entreprises d'investissements, membres des marchés réglementés d'instruments financiers, les personnes morales ayant pour objet principal ou unique l'activité de compensation d'instruments financiers, les personnes réalisant, contrôlant ou conseillant des opérations portant sur l'acquisition, la vente, la cession ou la location de biens immobiliers (les notaires en particulier), les représentants légaux et directeurs responsables de casinos (rappelons-nous les cybercasinos), les personnes se livrant habituellement au commerce ou organisant la vente de pierres précieuses, de matériaux précieux, d'antiquités et d'œuvres d'art.

TRACFIN rassemble les renseignements de nature à établir l'origine des sommes ou la nature des opérations faisant l'objet de la déclaration de soupçon. S'il ressort des analyses de la déclaration des indices de blanchiment de fonds (des faits susceptibles de relever du trafic de stupéfiants ou d'une activité criminelle organisée), TRACFIN transmet le dossier au parquet. Toutefois, la déclaration de soupçon ne figure pas au dossier de la procédure. En outre, une déclaration faite de

[144]Groupe d'Action Financière, créé à la suite du Sommet de l'Arche en 1989 qui réunissait les 7 pays les plus industrialisés. Le GAFI, basé en France à l'O.C.D.E, est chargé d'analyser la problématique du blanchiment, de formuler des recommandations (il y en a 40) et de procéder à des évaluations de ses adhérents pour vérifier les dispositifs de prévention et de lutte contre le blanchiment.

bonne foi ne peut engager la responsabilité du professionnel qui la fait. En cas de préjudice résultant directement d'une telle déclaration, l'Etat répond du dommage subi. Au fait, est-il judicieux et opportun de soumettre l'avocat à la déclaration de soupçon ?

b- La déclaration de soupçon : l'avocat devient-il un délateur de conjoncture ?

La question du secret professionnel de l'avocat et de l'inviolabilité du cabinet de l'avocat qui en résulte se heurte aujourd'hui à un argument de poids : la lutte contre le blanchiment d'argent sale. C'est une nécessité d'ordre public qui mobilise les pouvoirs publics. Aussi, la transparence des affaires qui semble être la solution apportée à ce fléau menace aujourd'hui le secret professionnel de l'avocat. Cependant, la difficulté de cette situation n'est pas seulement liée au fait qu'il s'agisse d'un professionnel soumis au secret, elle est surtout liée au fait que l'avocat soit un défenseur. Tout ceci renvoie à une approche rationnelle de la défense.

Au niveau européen, communautaire, on assiste à une remise en cause du secret professionnel de l'avocat. Pourtant une première remarque consiste à dire que même si les avocats peuvent se constituer en société, l'avocat n'est pas un commerçant. Il ne peut faire du commerce qui constitue le socle même du blanchiment d'argent. A ce propos et en matière de blanchiment, l'application des directives du 10 juin 1991 a donné lieu à discussions.

Aussi, la Commission européenne a-t-elle envisagée que la déclaration de soupçon puisse faire l'objet d'une distinction s'agissant des avocats, puisque *« la Commission concèderait que ceux-ci pourraient être exonérés de toute obligation en matière d'identification et d'information dans tous les cas liés à la représentation ou à la défense d'un client dans une procédure judiciaire »*.

La Commission envisage que les avocats soient autorisés à communiquer leurs soupçons en matière de blanchiment à leur Barreau ou à un organe profession équivalent plutôt qu'aux autorités anti-blanchiment.

Il existerait par conséquent une véritable obligation de délation qui s'avère effectivement être totalement contraire à la vocation de l'avocat, défenseur de la veuve et de l'orphelin, certes,

mais également du suspect démuni. Le fait que cette délation *« s'exerce auprès du Bâtonnier de l'ordre ne change rien à l'affaire »* ainsi que le soulignait le Vice-Président de l'UJA dans un article consacré à l'avocat et au blanchiment. Il faut comprendre que le Bâtonnier en ce moment là joue un rôle de censeur et non de défenseur, bien qu'il soit avocat avant tout.

L'Union des Jeunes Avocats (UJA) a consacré toute une réflexion à ce sujet et son vice-président, Eric DEZEUZE rappelait dans un article publié le 8 novembre 1999 que *« la mission, le rôle social de l'avocat dans une société démocratique sont à notre sens inconciliable avec toute fonction de dénonciation qui lui serait impartie y compris dans des domaines aussi sensibles et cruciaux que l'indispensable lutte contre les infractions les plus graves ou contre les organisations de type mafieux ou terroristes. Mais revendiquer en matière de blanchiment le fardeau qu'est le secret professionnel, impose à l'avocat des devoirs, une vigilance supplémentaire ».*

Si l'avocat ne peut être délateur, il ne saurait participer à un mécanisme de blanchiment, ou à une autre activité criminelle. Dans un autre article publié le 20 avril 2000, également dans les *Annonces de la Seine*, Frédéric NOUEL, Président de l'UJA de Paris et Patricia SAVIN, Secrétaire générale adjointe de l'UJA rappelaient que: *« le blanchiment des capitaux se fait sans les avocats ; une lutte efficace passe d'abord par une meilleure maîtrise des procédures légales d'obstruction dans l'espace de SCHENGEN ».*

Elle passe surtout par une volonté politique de cerner la question des paradis fiscaux. Elle passe certainement aussi par une définition étroite et précise enfin susceptible de permettre le respect du principe d'interprétation stricte de la loi pénale, de l'infraction de blanchiment dont l'un des paradoxes est de conférer l'apparence de la légalité à ce qui ne l'est pas ; dans ces conditions, s'attaquer à l'avocat - dernier maillon éventuel d'un processus très vaste impliquant les états eux-mêmes, ainsi que cela ressort, notamment, d'un rapport publié lundi 14 février 2000 par les 26 pays membres du Groupe du GAFI, ressemble à une faste opération de désinformation politique qui se fait aux dépens des libertés, sans même que l'intervention du juge ait été prévue. Cette situation préoccupante nécessite un combat commun des avocats et

des magistrats. C'est dans cette perspective que la publication du 'Livre blanc' contre le blanchiment a été décidée. La formation des avocats et leur assistance afin d'exercer leur vigilance concernant par le Barreau de Paris des opérations révélant un risque de blanchiment.

Le but poursuivi par le Conseil de l'Ordre étant de confirmer, dans son principe comme dans la lettre, le devoir de tout avocat qui doit consister, non pas à dénoncer mais à refuser de prêter son concours à toute opération de blanchiment, sauf à prendre le risque de se rendre complice de l'activité incriminable. Cependant, en dehors de toute discussion concernant la portée de la directive européenne, faire peser sur l'avocat cette obligation de déclaration apparaît d'autant plus surprenante, que l'obligation légale de dénonciation qui existe pour certaine catégorie de personne est, elle-même, fort peu respectée.

Il convient d'affirmer que dans une société qui se veut démocratique, la transparence doit être la règle et le secret l'exception. Ce secret ne peut qu'être réglementé; il l'est pour ce qui concerne l'avocat sur le plan légal ainsi que sur le plan déontologique comme nous l'avons étudié dans le premier chapitre de nos travaux.

En revanche, il en est tout à fait différemment pour ce qui concerne l'application de l'article 40 du Code de Procédure Pénale *« Toute autorité constituée, tout officier public ou fonctionnaire qui, dans l'exercice de ses fonctions, acquiert la connaissance d'un crime ou d'un délit est tenu dans donner avis sans délai au Procureur de la République et de transmettre à ce magistrat tous les renseignements, procès-verbaux et actes qui y sont relatifs »*.

Cette obligation est faite, non seulement aux fonctionnaires de Police mais à toutes les catégories de fonctionnaires de l'Etat, des régions, des départements et des communes. Or, ces prescriptions de l'article 40 du Code de Procédure Pénale, ne sont assorties d'aucune sanction pénale[145]. Par conséquent, des services aussi bien informés que ceux du Ministère des Finances, que ceux du Ministère de la Défense ou du Ministère de l'Intérieur, n'encourraient

[145] Cass. Crim. 13 octobre 1992 : Bull. Crim. n° 320

aucune sanction pour ne pas avoir respecté cette obligation de dénonciation. La situation de l'avocat n'est pas analogue. Il est *« détenteur du secret, non par privilège mais par obligation, se verrait, lui-même, soumis à cette obligation de dénonciation »*[146].

Pour Michel BEAUSSIER, Membre du Conseil de l'Ordre, qui représentait le Barreau de Paris à un colloque[147], l'avocat ne doit pas subir les contrecoups du blanchiment de fonds du trafic des stupéfiants ou de l'activité des organisations criminelles.

Il y a deux ans, un article publié au journal Libération, *« Argent sale : le Barreau de Paris s'accroche au secret des avocats »* faisait un grand bruit. L'auteur de cet article rappelait que le Barreau de Paris refusait l'extension de la déclaration de soupçon aux avocats. Il en va de la division sociale du travail, un avocat n'est pas un agent de renseignement de l'administration judiciaire. Ce n'est pas cela le sens commun du mot avocat. En même temps, il faut garder à l'esprit que l'avocat doit toujours faire montre d'une certaine probité morale.

b- De la cybersurveillance à la cyberperquisition ?

L'avocat peut-il se servir du secret professionnel à des fins criminelles ou délictuelles sans courir le risque de complicité et, par conséquent, exposer son cabinet à une perquisition ?

La perquisition dans un cabinet d'avocat est envisageable en cas de crime flagrant en application des articles 56 et 57 du Code de Procédure pénale. En l'occurrence, *« si la nature des crimes est telle que la preuve puisse en être acquise par la saisie de papiers, documents ou autres objets en la possession de personnes qui paraissent avoir participé au crime ou détenu des pièces ou objets relatifs au fait incriminé ».*

La cybersurveillance d'un cabinet d'avocat ou d'un autre professionnel qui est consécutive à la commission d'un acte criminel n'a rien de moins qu'une perquisition. L'esprit et la finalité des recherches étant les mêmes, il convient juste de replacer les méthodes dans leurs contextes. On

[146] Roland SANVITI, L'avocat face à deux mondialisations : les entreprises et les mafias, Editions Ediprim, 2001.
[147] Colloque « Blanchiment : tous complices », le samedi 18 mars 2000

peut parler de cyberperquisition qu'on peut définir chichement comme toute recherche et saisie de preuves informatiques relatives à un acte criminel aux fin d'une enquête judiciaire.

L'efficacité technique de cette méthode est qu'elle est possible de près et de loin. De près, dans le cabinet, en procédant à la saisie des outils informatiques, y compris les documents imprimés ; de loin, en accédant aux données en réseaux.

Le danger de cette cyberperquisition qui serait la fouille des dossiers archivés sur support numérique, réside dans le fait que les conditions de la perquisition d'un cabinet d'avocat ne peuvent être réunies (la présence du bâtonnier etc.). Pourquoi envisageons nous cette hypothèse ? L'un des moyens les plus sûrs de stockage de documents est de les envoyer par e-mail en « fichier attaché » sur une adresse créée à cette fin. Un professionnel soumis au secret peut se permettre une telle opération lorsqu'il estime avoir sécurisé son message (par le cryptage etc.). D'ailleurs, la LOPSI (II) présentement en cours de discussion a prévu cette cyberperquisition. Cette mesure vivement critiquée a été retirée, du moins pour le moment. Il est possible qu'elle soit reprise par la nouvelle *loi sur l'économie numérique*.

La cyberperquisition du cabinet virtuel peut avoir lieu à tout moment et dans n'importe quelles conditions (en procédant aux écoutes également). La perquisition du disque dur à distance, en notre présence mais à notre insu, est possible. Et puis, avec la loi du 13 mars 2000, la preuve informatique est définitivement admise en droit positif. La preuve informatique provenant d'une cyberperquisition est tout a fait recevable. Cette situation est à nuancer avec la cybersurveillance qui est essentiellement exploratoire.

On peut objecter qu'il n'y a pas de problème majeur si le professionnel n'a rien à cacher. Or, justement, il a tout à cacher. Il a l'obligation pénale de tout cacher sur ses affaires (art. 226-13 NCP). On ne peut pas poser une obligation et en empêcher l'accomplissement sans se contredire.

Aussi, faut-il noter que l'avocat français ne manie pas vraiment de fonds et semble préservé des risques de blanchiment du fait de l'existence de la CARPA (Caisse de Règlement Pécuniaire des Avocats), sous le contrôle exercé par l'Ordre des avocats.

Ce système qui a été mis en place à Paris en 1957, à l'initiative du Bâtonnier Claude LUSSAN, a été étendu aux autres barreaux progressivement. Il a été facultatif il est devenu obligatoire et définitif. C'est-à-dire qu'il existe un véritable cloisonnement entre les fonds qui peuvent soit provenir de l'issue d'un procès, soit de tout autre opération financière et qui sont placés sur la CARPA et les fonds reçus sous forme de frais ou d'honoraires par l'avocat sur son compte personnel. D'ailleurs, à l'instar des barreaux français, le Conseil des Barreaux de la Communauté Européenne s'en est inspiré sous la désignation «Fons des Clients» à l'article 3.1.8 du Règlement Intérieur.

De fait, avec la globalisation de la criminalité financière, les mesures nationales n'aboutiront que dans la mesure d'une harmonisation internationale contre ce fléau. Une anecdote racontée dans le rapport du SCPC (Service central de prévention de la corruption), relatant l'expérience d'un journaliste suisse témoigne de cette nécessité. Afin de tester les convictions éthiques des dix plus prestigieux cabinets d'avocats de Zurich (Suisse), l'homme s'installe dans une chambre d'un palace, en se faisant passer pour un homme d'affaires tchèque. Il contacte (par téléphone) dix cabinets en leur expliquant qu'il s'apprête à vendre un kilo d'osmium, un produit dangereux, qu'il a volé et qu'il a besoin de dissimuler 5 millions de dollars. Sans difficulté, chaque cabinet lui dépêche sur-le-champ un émissaire, et tous proposent de lui créer une société off-shore, aux îles Caïmans, à Panama, au Liechtenstein. Un avocat fait encore mieux, en proposant que les sommes transitent sur les comptes de son cabinet et en expliquant que si l'homme d'affaires avait du plutonium à vendre, il lui assurerait un transfert de fonds vers Dubaï, où l'avocat a de bons contacts....

La lutte contre le blanchiment de capitaux et le financement des activités terroristes est une des activités prioritaires de l'Union européenne. L'adoption de la proposition actualisant la directive relative au blanchiment de capitaux va représenter une avancée importante dans ce domaine (cf. IP/01/1608). L'adoption rapide de la directive sur les abus de marché (cf. IP/01/758 et MEMO/01/203) fournirait une autre base essentielle pour lutter contre l'utilisation illicite des systèmes financiers. L'Union européenne continuera à jouer un rôle considérable au sein du Groupe d'action financière (GAFI), l'organisation mondiale de lutte contre le blanchiment de capitaux. Des réflexions sont en cours sur des questions comme la surveillance du transport

international d'espèces et sur l'assouplissement des législations sur le secret bancaire, de sorte que les traces financières laissées par les terroristes puissent être repérées plus efficacement qu'aujourd'hui.

Tout ce qui peut compromettre l'indépendance et l'honorabilité de l'avocat semble porter également atteinte à l'essence même de sa profession.

2- <u>la cybersurveillance d'un auxiliaire de justice</u> : une présomption de culpabilité ou de complicité ?

« Je jure, comme avocat, d'exercer mes fonctions avec dignité, conscience, indépendance, probité et humanité » : le serment de l'avocat semble être un véritable engagement de bonne conduite envers la société. Plus qu'un engagement le serment est en réalité un pacte sacré auquel on ne déroge pas.

Le serment de l'avocat était un peu de même nature que l'ordination des prêtres car l'avocat prêtait serment sur la sainte Bible. Le serment avait une dimension spirituelle. D'autres y revoient les rites de l'Ancien Régime, le sacre en particulier. L'avocat qui était admis à la Cour partageait ainsi la foi et la dignité qui sont celles de la Justice. C'est peut-être pour cela qu'on les appelle aussi *« serviteurs de Thémis »*, comme s'ils étaient des justiciers.

En effet, Thémis est la déesse de la justice. Elle appartient à la lignée des dieux de la mythologie grecque. Elle est l'une des épouses de Zeus. Selon Homère, elle est la personnification des lois qui régissent la justice. Respectée par tous les dieux de l'Olympe, elle assiste aux délibérations des dieux et des hommes et préserve, en toute occasion, l'équité des décisions qui y sont prises. On la symbolise par une balance et une épée dans les mains ce qui constitue les deux emblèmes de la justice ; ses yeux bandés sont le symbole de l'impartialité des sentences qu'elle rend.

Jerold S. AUERBACH l'a mis en évidence : *« Le droit est notre religion nationale, les avocats sont notre clergé, les palais de justice nos cathédrales où les passions contemporaines sont représentées »*[148].

Un règlement du Parlement de Paris de 1344 qui énumère les engagements que doivent prendre les avocats précisait qu' *« exercer leur office, avec fidélité et exactitude, ne point se charger de causes injustes, s'abstenir de faire de fausses citations et d'alléguer des coutumes qui ne croiraient pas vraies, expédier les causes le plus tôt qu'il leur sera possible, sans chercher malicieusement, ou par des subterfuges, à se procurer des remises, de ne jamais réclamer au-delà de 30 livres parisis, étant à eux, cependant, permis de recevoir moins ; de rabaisser leurs salaires en raison de la modicité de la cause et de la médiocre condition des parties ; de ne faire aucun traité avec leur client sur l'événement du procès ».*

Ce rappel historique de Yves OZANAM, archiviste de l'Ordre des avocats à la Cour d'Appel de Paris, revêt d'une importance capitale : *« Puisque, effectivement, jusqu'à la révolution, le serment de l'avocat va se caractériser par une double dimension à la fois professionnelle et religieuse. Ainsi qu'il a été donné de l'aborder, la période révolutionnaire a été une parenthèse douloureuse pour la profession d 'avocat et le serment professionnel n'est réapparu qu'avec la renaissance d'une profession réglementée en 1804 ».*

Cependant, la notion de surveillance telle que nous l'avons abordée ne peut que revêtir un caractère intrinsèquement péjoratif lorsqu'elle s'applique à un auxiliaire de justice. En principe, l'avocat tout auxiliaire de justice qu'il est, prête serment pour 'gagner' la confiance de la société. La soumission à la surveillance ne s'apparente-t-elle pas à la 'profanation' de ce serment ?

La cybersurveillance semble être une atteinte à la dignité et à la probité de l'avocat. La cybersurveillance étant suspicieuse par nature, elle constitue une atteinte à la présomption d'innocence de l'avocat. Or le rôle de ce dernier est de faire en sorte que le droit fondamental qu'est la présomption d'innocence soit respecté, en tout état de cause. De là, la cybersurveillance de l'avocat ne peut que faire l'objet d'une perception négative.

[148] AUERBACH Jerold S., Justice without Law? Resolving Disputes without Lawyers, Oxford, 1983, page 9.

La Fédération des ordres professionnels de juristes du Canada (FOPJC) a contesté la validité de certaines dispositions de la Loi sur le recyclage des produits de la criminalité. Cette loi remet en question le secret professionnel des avocats qui sont désormais surveillés comme des délinquants potentiels.
La FOPJC estime qu'on ne peut à la fois obliger au secret et briser la confidentialité des dossiers en se fondant sur une suspicion générale.

Mais quels naïfs serions-nous à croire que l'avocat ne parle jamais de ses affaires ! Ne serait-ce qu'aux proches…On en voit de toutes sortes : du plus modeste au plus pédant.
En outre, la fonction de conseil de l'avocat n'est pas toujours 'divine'. Il n'est plus rare aujourd'hui rare de rencontrer des avocats d'affaires très doués en matière de blanchiment d'argent et qui sont complices de leurs clients. (Encore faut-il le prouver, et cela rapporte beaucoup !)
Il convient, encore une fois, de distinguer la fonction de conseil juridique de la fonction de défense. La protection de la deuxième fonction (la défense) est indispensable pour une bonne administration de la justice.

En revanche, l'avocat n'est pas obligé de tout mettre en ligne. Il n'est pas non plus obligé de saisir les informations sensibles sur quelque support qu'il soit.
Alors, cybersurveillance de l'avocat, pourquoi faire si ce n'est porter une atteinte gratuite à la profession?

Lorsque l'on se penche sur le secret bancaire, on s'aperçoit qu'il fait l'objet de plusieurs paradoxes. Ainsi, pouvons-nous remarquer une contradiction entre obligation de secret et celle d'informer qui pèse sur le même banquier. Les données personnelles qui forment le soubassement du secret bancaire, sont les objets d'investigation tant du fisc que de la police judiciaire selon les cas. En cela le secret bancaire qui est un secret professionnel diffère radicalement du secret médical. Quelle est donc la portée du privilège de confidentialité du banquier, au nom du secret auquel il est soumis ? Le secret bancaire, serait-il en définitive un secret résiduel ?

3- <u>Le secret bancaire</u> : un terrain important d'investigation, un secret résiduel ?

a- La déclaration de soupçon et le secret bancaire

Le principe est que les banques ne peuvent pas opposer le secret bancaire à la Banque de France, à la Commission bancaire et à l'autorité judiciaire agissant dans le cadre d'une procédure pénale. Exceptionnellement, il est prévu que le secret bancaire est levé lorsqu'une banque a un soupçon qu'elle se doit de déclarer à TRACFIN. Ainsi, une déclaration de soupçon n'entraîne pas la violation du secret bancaire.

L'intégration est l'étape que la cybersurveillance permet de déjouer dans un processus de blanchiment comme nous l'a expliqué un directeur d'une agence bancaire.

Cette étape consiste à conférer une apparence licite à des fonds d'origine criminelle. Pour reprendre les termes du GAFI (rapport 1989) : *« Une fois terminé le processus de l'empilage, le blanchisseur a besoin de fournir une explication pour habiller sa richesse d'un parfum de légalité. Les plans d'intégration replacent les produits blanchis dans l'économie de telle façon qu'ils réintègrent le système bancaire en apparaissant alors tels des profits normaux d'une affaire commerciale. A moins d'avoir pu établir la trace de profits illicites de façon formelle au cours des deux premiers stades du blanchiment, il va devenir extrêmement difficile de pouvoir distinguer les richesses légales des richesses illégales ».*

Les différentes méthodes sont les suivantes : les ventes de biens immobiliers, les sociétés écrans (notamment établis dans des paradis fiscaux et/ou dans lesquels le secret bancaire est important) et les emprunts fabriqués (entreprise se prêtant à elle-même les produits illicites blanchis par l'intermédiaire de sociétés écrans), la complicité des banques étrangères, les fausses factures en import-export ; ce système repose sur une surévaluation sur les documents d'entrée pour justifier des fonds déposés ensuite dans des banques ou une surévaluation des exportations pour justifier des fonds reçus de l'étranger.

La déclaration de soupçon est une limite à la confidentialité. Or la confidentialité est ce qui fait la sécurité et le succès d'une entreprise bancaire.

c- La confidentialité comme sécurité bancaire

Selon Michel DERROBERT, la discrétion est « un pilier » du succès des banques suisses[149]. Les banquiers suisses ont l'obligation de garder strictement confidentielle toute information sur vous et votre compte.

Ce secret bancaire, parmi les plus stricts du monde, est une tradition à l'histoire fort ancienne. Il est consacré dans la loi suisse. Un banquier qui révélerait des informations à votre sujet sans votre consentement risque des mois de prison.

Les seules exceptions à cette règle concernent les crimes graves (trafic d'armes, trafic de drogue).

Le secret bancaire n'est pas levé dans les cas d'évasion fiscale. En effet, l'omission de déclarer certains revenus ou actifs n'est pas un crime en Suisse. Ainsi, ni le gouvernement suisse, ni aucun autre gouvernement ne peut obtenir des informations sur votre compte bancaire. Ils doivent d'abord convaincre un juge suisse que vous avez commis un crime grave puni par le code pénal suisse.

Les premiers clients des banquiers suisses étaient les rois de France - et ceux-ci appréciaient principalement la discrétion de leurs bâilleurs de fonds. En effet, les banquiers genevois étaient protestants, souvent d'origine française chassés par la révocation de l'édit de Nantes par Louis XIV en 1685. Oubliant les persécutions dont ils avaient été victimes en France, ils continuèrent à financer le roi de France depuis Genève. Mais il faut dire qu'à l'époque, il n'y avait pas meilleur emprunteur que le roi. Celui-ci avait à la fois la capacité de rembourser ses emprunts et des besoins insatiables de financement. La discrétion avait une importance cardinale, car il ne pouvait être dit que le roi empruntait à des hérétiques protestants.

L'un des premiers textes qui règle formellement le secret bancaire date de cette époque : le Grand Conseil Genevois adoptait en 1713 le premier texte connu sur le secret bancaire. Il s'agissait d'une réglementation de l'activité des banques qui précise que les banquiers doivent *« tenir un*

[149] Les origines historiques du secret bancaire suisse, http://switzerland.isyours.com

registre de leur clientèle et de leurs opérations, mais il leur est interdit de divulguer ces informations à quiconque autre que le client concerné, sauf accord exprès du Conseil de la Ville».

Par la suite, la Suisse devint un véritable 'asile financier et politique' à ceux qui fuyaient la tourmente politique qui déchira le continent depuis 1789, offrant un refuge salutaire aux capitaux des nobles qui redoutaient la Révolution, et aux divers gouvernements qui se succédèrent durant le XIX ème siècle.

Les banquiers genevois étaient banquiers des rois de France… Louis XVI avait même un banquier suisse comme ministre des finances, Necker. Napoléon lui-même était un client assidu d'une banque suisse.

Le secret bancaire apparaît comme un élément important du droit au respect de la vie privée.

Les bases de données du banquier contiennent le nom, l'adresse…bref, toute l'identité bancaire du client. Celles-ci permettent non seulement d'effectuer des opérations (transferts de fonds et autres transactions), mais surtout la fortune personnelle sont des données protégées relatives à l'intimité de la vie privées et par conséquent protégées par l'article 9 du Code civil cité plus haut.

c- La cybersurveillance et les données bancaires

Le banquier gère ainsi des données personnelles qui doivent être tenues confidentielles parce que relevant de la vie privée. La protection de la vie privée semble être le fondement du secret bancaire. Michel DEROBERT s'est préoccupé de la confidentialité des données bancaires à caractère personnel dans un célèbre article publié dans *Le Temps* des 8 et 9 janvier 2000 : *« L'homme transparent ou la fin de la sphère privée ».* Un bref stage dans le secteur bancaire nous a permis de découvrir que le système bancaire est complètement informatisé.

La cybersurveillance permet à la police d'effectuer des investigations sur les transferts de fonds dans le secteur financier. Elle constitue selon un directeur de banque un *« outil essentiel de contrôle fiscal moderne ».*

Dans cet article l'auteur s'inquiétait du fait que des données relatives aux comptes et aux opérations bancaires des clients soient divulguées. En principes, en tant que données liées à la vie privée des clients et protégées par le secret bancaire, ces données ne peuvent être ni connues des tiers, ni divulguées. Or *« grâce à l'aide d'employés de banque peu scrupuleux,* écrit Michel DERORBERT, *un détective a pu se procurer des données protégées par le secret bancaire. Les suites ne se sont pas fait attendre : des personnes ont été licenciées, d'autres écrouées, l'appareil judiciaire a été mis en branle et l'enquête pénale suit son cours »*. Dans une conférence publiée[150] le banquier soutenait que la sécurité et la confidentialité est ce que vont chercher les clients auprès des banques suisses.

La confidentialité des opérations bancaires est souvent brisée pour faciliter l'accès aux dossiers des clients par le fisc et la police judiciaire. Le secret bancaire qui n'est pas opposable au fisc ne porte pas en lui une marque véritable de privilège de confidentialité. Il n'est donc qu'un secret résiduel.

Il est bien connu que la COB, le fisc et les douanes luttent également contre le terrorisme.

Ainsi le volet très sécuritaire et complètement liberticide de la loi sur la sécurité quotidienne, qui a une durée temporaire jusqu'en 2003 (parce que parait il que la France serait actuellement "menacée de terrorisme") vient d'être encore renforcé.

Le 5 décembre dernier, dans le cadre de la loi de finances rectificative pour 2001, un amendement a été adopté sans débat pour que la COB, le fisc et les douanes accèdent aux données de connexion des fournisseurs d'accès. (Voir article 32 bis, fin page 8 et début, p. 9)

Ils pourront aussi pénétrer dans les locaux des opérateurs de télécoms, mêmes si ces derniers sont des personnes physiques (il suffit de transmettre les données d'un tiers pour être considéré comme opérateur de télécommunication)

[150] Michel DERORBERT, Le secret bancaire et l'emploi à Genève, 10 mai 2001, p.16, pp.6 http://www.genevaprivatebankers.com/fr/10mai2001.

C'est totalement scandaleux et contraire à la constitution (article 66 : autorité judiciaire gardienne de la liberté individuelle).
De plus, alors que l'article L 32-3-1 du code des postes et télécommunications introduit par la loi LSQ, dit que les données de connexion ne doivent être effacées qu'au bout d'un an pour "la mise à disposition de l'autorité judiciaire d'informations" dans le cadre de poursuites pénales.
Le gouvernement soutenait que ce texte n'était qu'une confirmation de l'interprétation de la loi (Florence PARLY à l'Assemblé le 05/12/2001 : *« tend à confirmer les pouvoirs légaux conférés pour les besoins de leurs missions à la douane, à la direction générale des impôts et la COB ».* En effet, un article de la loi sur la sécurité quotidienne avait pu créer un a contrario, source d'imprécision et de contentieux). Alors que le terme « autorité judiciaire » est très clairement défini comme la justice indépendante par la constitution (article 64 : *« Le Président de la République est garant de l'indépendance de l'autorité judiciaire. »*).

Il s'agit donc bien des magistrats du siège, pas du parquet et encore moins de la police.

Un autre problème se pose quant à la compatibilité des lois : quels sont les conséquences des lois anti-blanchiments sur les lois informatique et liberté et quelle est la position de la CNIL à ce sujet?
Il y a effectivement incompatibilité entre ces lois dans la mesure où le banquier qui déclare un soupçon ne doit pas en informer le client qui en fait l'objet sous peine d'une amende (sanction pénale) de 15 à 150 KF; c'est contradictoire avec le droit d'accès aux fichiers imposé par la CNIL. Cependant, la CNIL ne semble pas prendre position quant à un aménagement ou pour trouver une solution. Des décrets d'application de la loi sur les Nouvelles Régulations Economiques particulièrement s'agissant des opérations pour compte propre et pour compte de tiers avec un tiers enregistré ou domicilié dans un Pays et Territoire Non Coopératif. Un décret a été pris en février 2002 imposant aux banques de déclarer à TRACFIN toutes les opérations d'un montant supérieur à 8.000 EUR avec NAURU. Pour être complet, la Commission bancaire a diffusé le 28 mars 2002 une instruction précisant certaines notions donneuses d'ordre, bénéficiaires, fonds fiduciaire).

Le système de l'endossement s'est révélé un système de blanchiment d'argent criminel. Le rapport du député socialiste Arnaud MONTBOURG[151] est particulièrement instructif à cet égard.

La cybersurveillance est vraisemblablement un moyen efficace de lutte contre les systèmes mafieux de blanchiment d'argent. Ce faisant, il est impératif de protéger le système bancaire de sorte à garantir la vie privée et le secret bancaire qui n'est pas pour autant officiellement aboli.
Il convient de revenir sur une question d'actualité : faut-il surveiller les surveillants ?

4-Le double degré de surveillance : la question de la surveillance des cybersurveillants

Les conclusions sur la surveillance des salariés sur leur lieu de travail présentées par la CNIL le 11février 2002 fait suite à la consultation des instances syndicales et patronales qu'elle avait initiées en mars dernier.

La CNIL a considéré qu' *« une interdiction générale et absolue de toute utilisation d'Internet à des fins autres que professionnelles ne paraît pas réaliste ».* Il convient subséquemment d'en préciser les limites.

Les modalités d'un contrôle *a posteriori* des données de connexion doit faire l'objet d'une consultation du comité d'entreprise ou du comité technique paritaire le cas échéant. Dans le cas d'un contrôle individualisé, le dispositif contrôlant les durées de connexion et les sites visités doit être déclaré à la CNIL. Cette dernière propose une limitation de la durée de conservation de six mois. Rappelons qu'elle proposait une durée maximale de trois mois pour une consultation à des fins judiciaires.

Les e-mails échangés sur le lieu de travail sont considérés comme étant professionnels sauf s'ils

[151] Le rapport " Montebourg ", Rapport parlementaire, Assemblée Nationale, Avril 2002 pour la France

sont rangés dans un répertoire destiné à un usage privé ou si leur objet fait mention d'un caractère clairement privé. C'est donc uniquement dans ces derniers cas que le secret des correspondances peut être préservé.

Cette instance à but consultatif pose aussi la question du statut des administrateurs de réseaux. Dans le cadre de leurs fonctions, ils sont amenés à avoir accès à l'ensemble des informations relatives aux utilisateurs (messageries, durée et fréquence de connexion etc.).

La CNIL leur réserve un droit au secret professionnel dont ils pourraient faire usage pour s'opposer à la divulgation des informations non destinées à la sécurité à leur hiérarchie. La CNIL propose en outre la désignation d'un délégué à la protection des données dans les entreprises où l'effectif le justifierait. Il serait un correspondant *"informatique et libertés dans l'entreprise"*. Le statut de ces médiateurs n'est toutefois pas précisé dans le rapport.

Enfin, un bilan annuel *« informatique et libertés »* est préconisé. Lequel bilan devrait porter sur les mesures de sécurité qui ont conduit à conserver une trace de l'activité et de l'usage des utilisateurs.
Au niveau de l'Europe se met en place surveillance des logiciels d'espionnage. En effet, les instances européennes sont décidées à faire la chasse aux *spywares*. Ces logiciels dits « logiciels espions » qui sont installés à l'insu des utilisateurs portent naturellement atteintes à la vie privée des internautes.

Les *spywares* (ou « logiciels espions ») sont, par conséquent, illégaux en droit européen tout comme en droit français sur la protection de la vie privée et des données personnelles.
En outre, ces programmes, souvent installés à l'insu des utilisateurs sur des logiciels grand public, renseigneraient les éditeurs sur les habitudes des internautes.

Selon des informations rapportées par le *Wall Street Journal*, un groupe de travail composé de représentants d'organismes de régulation européens se pencherait actuellement sur les *spywares* inclus dans des lecteurs de fichiers multimédias, comme Windows Media Player, de Microsoft, ou RealJukeBox, de Real Networks.

La somme de ces études aurait été adoptée le 30 mai dernier, et pointerait des irrégularités par rapport aux lois en vigueur dans l'Union européenne (UE).

Le double degré de surveillance est à la fois une garantie contre l’atteinte illégale à la vie privée et une garantie à la sauvegarde du secret professionnel.

Conclusion :

Cette étude a pour point de départ le constat d'un paradoxe : tout en affirmant solennellement la liberté de communication, le législateur a choisi d'en aménager les conditions d'exercice de façon particulièrement restrictive. Tout en imposant le secret dans le cadre de certaines professions, le législateur décide de tout savoir, contraignant parfois ceux à qui il a imposé le secret à la divulgation active ou passive.

Dans la logique juridique, Nouvelle rhétorique, Dalloz 1976, Perelman pensait pour sa part que le droit doit satisfaire à une double exigence : l'une d'ordre logique qui impose la nécessité d'une cohérence de l'ordre juridique, l'autre, d'ordre pragmatique, qui requiert, pour susciter l'adhésion, son caractère juste et raisonnable. Où en sommes-nous ?

Au-delà des conséquences concrètes de la cybersurveillance et du secret professionnel, il faut surtout prendre en compte leurs effets symboliques et leur dimension théorique. Ce qui mène à s'interroger sur l'attitude à observer face à des mesures qui portent des atteintes plutôt graves aux libertés et droits fondamentaux, de sorte à altérer l'idée qu'on se fait d'un Etat de droit. Or le maintien de l'ordre public et de la sûreté de l'Etat semblent souvent justifier ces atteintes.

« Salux populis, suprema lex » : le salut du peuple est la loi suprême.

Le secret est relatif dans le contexte actuel. La confidentialité s'inscrit désormais dans une dimension plus subjective Elle va de la non divulgation à la non généralisation des informations. 'Tout le monde ne doit pas être au courant. Quelques personnes peuvent savoir en faisant comme si de rien n'était. Parce que la loi les oblige à faire comme si de rien n'était.

Les défenseurs de la vie privée rappellent souvent la réplique du président américain Thomas Jefferson : *« Si tu es prêt à sacrifier un peu de liberté pour te sentir en sécurité, tu ne mérites ni l'une ni l'autre ».*

1-La cybersurveillance : une atteinte aux libertés de communication

Un équilibre entre le secret professionnel et la sécurité publique s'impose. L'histoire politique ne permet pas que l'on puisse donner 'carte blanche' à l'Etat en matière de libertés publiques, qu'il soit un Etat légitime ou non.
La confidentialité est intimement liée au respect de la vie privée et reste un droit fondamental qu'il convient de préserver. Le caractère démocratique et respectueux des libertés d'un Etat doit être l'objet d'un empirisme et d'un contrôle continu. La liberté ne se présume pas, elle se vit.

2- La vigilance est la condition des libertés individuelles face à la cybersurveillance

La vigilance du citoyen face à la cybersurveillance devient un impératif, peu importe qu'il soit tenu au secret professionnel, à moins de renoncer catégoriquement à la vie privée. Il importe, comme l'a d'ailleurs souligné Bilo Varen, de *« se tenir en garde contre les vertus mêmes des hommes qui occupent les postes les plus imminents ».*

La systématisation de la cybersurveillance semble faire de la CNIL un 'censeur d'employeurs indiscrets'. Aussi, tout porte à croire que son statut de garant de 'libertés publiques' est à reconsidérer.

Enfin, la cybersurveillance entraîne-t-elle une remise en cause ou alors une redéfinition du secret professionnel ?

BIBLIOGRAPHIE :

OUVRAGES :

AARNIO A., *Le Rationnel comme raisonnable, la Justification en droit*, LGDJ, 1992

BARTHELEMY J., *Temps de travail et temps de repos, l'apport du droit communautaire*, Droit Social janvier 2001, P.634

BENSOUSSAN A., *Informatique et télécoms*, éd. Francis Lefebvre, 1997, p.895

BENSOUSSAN A., *Informatique et télécoms*, éd. Francis Lefebvre, 2000

BOCHURBERG L., *Internet et commerce électronique*, 1re éd. DELMAS 1999, pp.135-151

DERIEUX E., *Droit de la communication*, L.G.D.J, 1999, 3e éd.

Docteur BRAOUARDEL P., *Le secret médical*, Baillière, Paris, 2e éd., 1993

DEJEAN Ph., *Puissance publique et sécurité des réseaux* in *Les nouvelles pratiques liées aux technologies de la communication*, actes des 10 journées organisées par le Magistère en Droit de la communicatique, éd. PUF, 1999, pp.123-130

DOSTOIEVSKI F., *Crimes et Châtiments*, Paris, Flammarion, 1984.

DERORBERT M., *Le secret bancaire et l'emploi à Genève*, 10 mai 2001, p.16, pp.6

De la Fontaine J., *Les Femmes et le Secret.*

FLORIOT R. et COMBALDIEU R., *Le secret professionnel*, Flammarion, 1973

FERAL-SCHUHL Ch., *Le droit à l'épreuve de l'Internet,* 3è éd. DUNOD 1999, p.353

FAVENNEC-HERY F., *Le temps de repos, une nouvelle approche du droit du travail*, RJS12/1999

HACKFORD T., *L'associé du diable*, livre aux éditions Pocket, 1997

HAMPATE-BÂ H., *L'étrange destin de Wangrin*

KELSEN H., *Théorie pure du droit*, traduit par Charles Eisenmann, LGDJ, 1999

LECLERCQ P., *La CNIL, garante de la finalité, de la loyauté et de la sécurité des données personnelles*, in Les libertés individuelles à l'épreuve des NTIC, (études réunies sous la direction de PIATTI Marie-Christine), éd. Presse Universitaire de Lyon (PUL), 2001

LUCAS A., DEVEZE Jean, FRAYSSINET Jean, *Droit de l'informatique et de l'Internet*, Thémis, novembre 2001, p.748

MICHAUT F., TROPER M., GRZEGORCZYK Ch., *Le positivisme juridique*, Paris : LGDJ, 1992

NICOLEAU P., *Lexique de droit privé*, ellipses, 1996

PIATTI M-Ch., *Les libertés individuelles à l'épreuve des NTIC* (études réunies sous la direction de PIATTI M-Ch.), éd. Presse Universitaire de Lyon (PUL), 2001, p. 211

PRADEL J., *Procédure pénale,* Cujas, 10^{e} éd., 2000/2001, pp.361-363

RAY J. E., *Le temps de travail des cadres*, Droit Social, mars 2001

RAY J. E., *Droit du travail et NTIC*, Droit Social novembre 2001

WAQUET Ph., *Le temps de repos,* Droit social, mars 2000

WAQUET Ph., *Le pouvoir de direction et les libertés des salariés*, Droit social, décembre 2000, p. 1051

Juges, *La Bible de Jérusalem*, chapitre 16, Les Éditions du Cerf 1997

Proverbe XXV, *La sainte Bible*, 9-10, Nouvelle Edition de Genève 1979, pp.629-659

Encyclopoedia universalis 1990, *Le secret professionnel* Encyclopoedia universalis France éditeur à Paris, p. 3170

MEMOIRES :

SANVITI, *L'avocat face à deux mondialisations : les entreprises et les mafias*, Editions Ediprim, 2001.

THESES :

MUTEAU Ch., *Du secret professionnel*, de son étendue et de la responsabilité qu'il entraîne, Paris 1870

DOCTRINE :

AUERBACH J.S., *Justice without Law? Resolving Disputes without Lawyers*, Oxford, 1983, page 9.

LE POITTEVIN G., note au S., 1897.I.81, sous Req. 9 avril 1895.
MONZEIN P., *Réflexion sur le secret médical*, D.1984, chron. P.9

PLANIOL M., note au D., 1899.I.585, sous Civ., 1er mai1899

ROUX J.A., note au S., 1914.I.169, sous Crim., 9mai 1913

SIMITIS S., *Les données sensibles revisitées*, consultable sous http://www.legal.coe.int

VIALA A., *Grenoble II, L'interprétation du juge dans la hiérarchie des normes et des organes,* http://www.conseil-constitutionnel.fr/cahiers/ccc6/viala.htm

RAPPORTS :

CNIL, *Rapport juin 2000* « *la cybersurveillance du salarié »,* Rapport 28 mars 2001

CNIL, *22e rapport d'activité 2001, éd. 2002*, La documentation Française

Le rapport " Montebourg ", Rapport parlementaire, Assemblée Nationale, Avril 2002 pour la France

Ordre national des médecins, *Commentaires du Code de déontologie médicale*, 1996, pp. 53-255

PERIODIQUES

Numéros spéciaux :

Droit Social juin 1992, *« Le droit du travail à l'épreuve des nouvelles technologies »*

Droit Social mars 2000, *« La loi Aubry II »*

Droit Social, janvier 2002 (à paraître), *« Droit du travail et nouvelles technologies de l'information et de la communication »*

Thibault Verbiest, *Terrorisme et Internet: vers une dérive sécuritaire*, 25 mars 2002

SITES INTERNET :

www.cnil.fr Commission Nationale Informatique et Liberté

www.courdecassation.fr Site officiel de la Cour de cassation

www.droit-technologie.org

www.ilo.org Organisation Internationale du Travail

www.legalis.net 'mensuel du droit de l'informatique et du multimédia'

www.tripalium.fr 'législation sociale et ressources humaines'

http://www.ecla.org/fr/objectifs/nationales.htm

http://www.liberation.fr/quotidien/portrait

Annexes :

Les amendements n° 9 ; 10 ; 11 ; 12 de la LSQ

PROJET DE LOI
SECURITE QUOTIDIENNE
(nouvelle lecture)

6 octobre 2001

AMENDEMENT N° 9

Présenté par

LE GOUVERNEMENT

_____

ARTICLE ADDITIONNEL APRÈS L'ARTICLE 6 TER

Après l'article 6 ter, insérer un article additionnel ainsi rédigé:

I- Il est inséré, après l'article L. 32-3 du code des postes et télécommunications, deux articles L. 32-3-1 et L. 32-3-2 ainsi rédigés

"Art. L. 32-3-1. - I.- Les opérateurs de télécommunications, et notamment ceux mentionnés à l'article 43-7 de la loi n° 86-1067 du 30 septembre 1986 relative à la liberté de communication, 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 Il, III et IV ci-après.

“ Il. - 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.

“III. - Pour les besoins de la facturation et du paiement des prestations de télécommunications, les opérateurs peuvent, jusqu'à la fin de la période au cours de laquelle la facture peut être légalement contestée ou des poursuites engagées pour en obtenir le paiement, utiliser, conserver et, le cas échéant, transmettre à des tiers concernés directement par la facturation ou le recouvrement, les catégories de données techniques qui sont déterminées, dans les limites fixées par le IV, selon l'activité des opérateurs et la nature de la communication, par décret en Conseil d'Etat, pris après avis de la Commission nationale de l'informatique et des libertés.

“Les opérateurs peuvent en outre réaliser un traitement de ces données en vue de commercialiser leurs propres services de télécommunications, Si les usagers y consentent expressément et pour une durée déterminée. Cette durée ne peut, en aucun cas, être supérieure à la période correspondant aux relations contractuelles entre l'usager et l'opérateur.

“IV. - Les données conservées et traitées dans les conditions définies aux Il et III portent exclusivement sur l'identification des personnes utilisatrices des services fournis par les opérateurs et sur les caractéristiques techniques des communications assurées par ces derniers.

“Elles ne peuvent en aucun cas porter sur le contenu des correspondances échangées ou des informations consultées, sous quelque forme que ce soit, dans le cadre de ces communications.

“La conservation et le traitement de ces données s'effectuent dans le respect des dispositions de la

loi n° 78817 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

“Les opérateurs prennent toutes mesures pour empêcher une utilisation de ces données à des fins autres que celles prévues au présent article.

“Art. L. 32-3-2. - La prescription est acquise, au profit des opérateurs mentionnés aux articles L. 33-1, L. 34-1 et L. 34-2, pour toutes demandes en restitution du prix de leurs prestations de télécommunications présentées après un délai d'un an à compter du jour du paiement.

“La prescription est acquise, au profit de l'usager, pour les sommes dues en paiement des prestations de télécommunications d'un opérateur appartenant aux catégories visées au précédent alinéa lorsque celui-ci ne les a pas réclamées dans un délai d'un an courant à compter de la date de leur exigibilité.”

Il- Il est rétabli, dans le même code, un article L. 39-3 ainsi rédigé:

“Art. L. 39-3. - I. - Est puni d'un an d'emprisonnement et de 75 000 euros d'amende le fait pour un opérateur de télécommunications ou ses agents:

“1° De ne pas procéder aux opérations tendant à effacer ou à rendre anonyme les données relatives aux communications dans les cas où ces opérations sont prescrites par la loi

“ 2° De ne pas procéder à la conservation des données techniques dans les conditions où cette conservation est exigée par la loi.

“Les personnes physiques coupables de ces infractions encourent également l'interdiction, pour une durée de cinq ans au plus, d'exercer l'activité professionnelle à l'occasion de laquelle l'infraction à été commise.

“Il - Les personnes morales peuvent être déclarées responsables pénalement, dans les conditions prévues par l'article 121-2 du code pénal, des infractions définies au I.

“Les peines encourues par les personnes morales sont:

“1° L'amende, suivant les modalités prévues par l'article 131-38 du code pénal;

“ 2° La peine mentionnée au 2° de l'article 13 1-9 du code pénal, pour une durée de cinq ans au plus;

“ 3° La peine mentionnée au 9° de l'article 31-39 du code pénal.

“L'interdiction mentionnée au 20 de l'article 13 1-9 du code pénal porte sur l'activité professionnelle dans l'exercice ou à l'occasion de l'exercice de laquelle l'infraction a été commise.”

OBJET

Les événements récents ont démontré que l'utilisation des moyens de télécommunications, des réseaux numériques et de l'Internet étaient au cœur des échanges d'informations entre les membres d'un réseau terroriste. Les données techniques relatives à ces communications sont autant de “traces ” laissées par les intéressés dans le monde virtuel, comme le seraient des empreintes ou des indices dans le monde réel. La recherche des infractions commises sur les réseaux de télécommunications ou à l'aide de ces réseaux suppose donc que puissent être exploités par les services d'enquête les données enregistrées par les opérateurs à l'occasion de l'établissement des communications émises par les auteurs de ces infractions. Il est nécessaire que la France se dote, à cet égard, d'un cadre législatif clair et transparent encadrant strictement ma conservation des données techniques à cette fin, de manière à ce que les autorités judiciaires ne soient pas tributaires des données conservées par les opérateurs pour leurs besoins propres, selon les choix commerciaux qu'ils auront fait. Cela impose de revoir l'ensemble du dispositif relatif aux obligations des opérateurs.

En effet, en vertu de la directive 97/66/CE du 15 décembre 1997 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications, les opérateurs de télécommunication ont, en principe, l'obligation de d'effacer ou de rendre anonyme l'ensemble des données dont ils disposent dès que la communication est terminée. C'est l'objet du I de l'article L. 32-3-1 nouveau du code des postes et télécommunications de consacrer ce principe. Ce ne peut être que, par voie d'exception, que des données sont susceptibles d'être conservées, notamment pour les besoins liés à la facturation par les opérateurs eux-mêmes de leurs services ou, selon les termes de l'article 14 de la directive, lorsque cela “constitue une mesure nécessaire pour sauvegarder la sûreté de l'Etat, la défense, la sécurité publique, la prévention, la recherche, la détection et le poursuite d'infractions pénales...

Le II de l'article L. 32-3-1 vise ainsi les données techniques susceptibles d'être exploitées pour les besoins de la recherche et de la poursuite des infractions pénales, étant précisé que les données techniques ainsi visées ne pourront être transmises qu'aux autorités judiciaires, dans le cadre d'une procédure pénale.

Cette obligation pèsera sur tous les opérateurs de télécommunications au sens du 150 de l'article L. 32 du code des postes et télécommunications, c'est-à-dire les prestataires qui assurent la transmission d'une communication. S'agissant de l'Internet, ce champ d'application inclut donc les fournisseurs d'accès, étant entendu que, pour leur part, les fournisseurs de services dit d'hébergement sont déjà assujettis, en application de l'article 43-9 de la loi du 30 septembre 1986 relative à la liberté de communication, dans sa rédaction issue de la loi du I er août 2000, à l'obligation de détenir et de conserver “les données de nature à permettre l'identification de toute personne ayant contribue. à la création d'un contenu des services dont (ils) sont prestataires”.

Dans les deux cas, les données techniques concernées seront précisément énumérées, selon l'activité de l'opérateur et la nature de la communication, par un décret en Conseil d'Etat pris avis de la Commission nationale de l'informatique et des libertés, étant entendu que ces données ne pourront en aucun cas porter sur le contenu des correspondances échangées ou des informations consultées.

L'article L. 39-3 nouveau du code des postes et télécommunications détermine le régime de l'infraction pénale qui sanctionne la méconnaissance des obligations posées par l'article précédent, concernant tant le principe d'effacement que l'obligation subsidiaire de conservation.

PROJET DE LOI
SECURITE QUOTIDIENNE
(nouvelle lecture)

6 octobre 2001

AMENDEMENT N° 10

Présenté par

LE GOUVERNEMENT

_____

ARTICLE ADDITIONNEL APRÈS L'ARTICLE 6 TER

Après l'article 6 ter, insérer un article additionnel ainsi rédigé:

Après l'article 230 du code de procédure pénale, il est inséré un titre Iv ainsi rédigé:

“TITRE IV

“DISPOSITIONS COMMUNES

“CHAPITRE UNIQUE

“De la mise au clair des données chiffrées nécessaires à la manifestation de la vérité

“Art. 230-I.- Sans préjudice des dispositions des articles 60, 77-1 et 156, lorsqu'il apparaît que des données saisies ou obtenues au cours de l'enquête ou de l'instruction ont fait l'objet d'opérations de transformation empêchant d'accéder aux informations en clair qu'elles contiennent ou de les comprendre, le procureur de la République, la juridiction d'instruction ou la juridiction de jugement saisie de l'affaire peut désigner toute personne physique ou morale qualifiée, en vue d'effectuer les opérations techniques permettant d'obtenir la version en clair de ces informations ainsi que, dans le cas où un moyen de cryptologie a été utilisé, la convention secrète de déchiffrement, Si cela apparaît nécessaire.

“Si la peine encourue est égale ou supérieure à deux ans d'emprisonnement et que les nécessités de l'enquête ou de l'instruction l'exigent, le procureur de la République, la juridiction d'instruction ou la juridiction de jugement saisie de l'affaire peut prescrire le recours aux moyens de l'Etat soumis au secret de la défense nationale selon les formes prévues au présent chapitre.

“Art. 230-2. - Lorsque le procureur de la République, la juridiction d'instruction ou la juridiction de jugement saisie de l'affaire décident d'avoir recours, pour les opérations mentionnées à l'article 230-i, aux moyens de l'Etat couverts par le secret de la défense nationale, la réquisition écrite doit être adressée au service national de police judiciaire chargé de la lutte contre la criminalité liée aux technologies de l'information, avec le support physique contenant les données à mettre au

clair ou une copie de celui-ci. Cette réquisition fixe le délai dans lequel les opérations de mise au clair doivent être réalisées. Le délai peut être prorogé dans les mêmes conditions de forme. A tout moment, l'autorité judiciaire requérante peut ordonner l'interruption des opérations prescrites.

“Le service de police judiciaire auquel la réquisition a été adressée transmet sans délai cette dernière ainsi que, le cas échéant, les ordres d'interruption, à un organisme technique soumis au secret de la défense nationale, et désigné par décret.

“Art. 230-3.- Dès l'achèvement des opérations ou dès qu'il apparaît que ces opérations sont techniquement impossibles ou à l'expiration du délai prescrit ou à la réception de l'ordre d'interruption émanant de l'autorité judiciaire, les résultats obtenus et les pièces reçues sont retournés par le responsable de l'organisme technique au service de police judiciaire qui lui a transmis la réquisition. Sous réserve des obligations découlant du secret de la défense nationale, les résultats sont accompagnés des indications techniques utiles à la compréhension et à leur exploitation ainsi que d'une attestation visée par le responsable de l'organisme technique certifiant la sincérité des résultats transmis.

“Ces pièces sont immédiatement remises à l'autorité judiciaire par le service national de police judiciaire chargé de la lutte contre la criminalité liée aux technologies de l'information.

“Les éléments ainsi obtenus font l'objet d'un procès-verbal de réception et sont versés au dossier de la procédure.

“Art. 230-4. - Les décisions judiciaires prises en application du présent chapitre n'ont pas de caractère juridictionnel et ne sont susceptibles d'aucun recours.

“Art. 230-5. - Sans préjudice des obligations découlant du secret de la défense nationale, les agents requis en application des dispositions du présent chapitre sont tenus d'apporter leur concours à la justice. ”

OBJET

La transmission de messages cryptés par la voie de l'internet s'est révélée être une forme privilégiée de communication entre membres d'un réseau terroriste. Dans les cas les plus sophistiqués de cryptologie, le déchiffrement de ces messages suppose d'avoir recours à des experts de très haut niveau voire à des moyens d'Etat couverts par le secret de la défense nationale. Il est nécessaire d'organiser le recours à ces moyens de manière à assurer leur fiabilité juridique dans le cadre d'une procédure pénale.

A cet effet, les articles 230-I à 230-5 nouveaux du code de procédure pénale prévoient la possibilité pour les autorités judiciaires de saisir l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication qui sera chargée de transmettre la demande de déchiffrement à un centre technique d'assistance placée sous l'autorité du ministre de l'intérieur. Les résultats devront être communiqués au magistrat compétent par la même voie, accompagnés des indications techniques utiles à leur compréhension et à leur exploitation, dans le respect, toutefois, des obligations découlant du secret de la défense nationale.

PROJET DE LOI
SECURITE QUOTIDIENNE
(nouvelle lecture)

6 octobre 2001

AMENDEMENT N° 11

Présenté par

LE GOUVERNEMENT

_____

ARTICLE ADDITIONNEL APRÈS L'ARTICLE 6 TER

Après l'article 6 ter, insérer un article additionnel ainsi rédigé:

Il est inséré, après l'article Il de la loi n° 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des télécommunications, un article Il I ainsi rédigé:

"Art. 11-1.- Les personnes physiques ou morales qui fournissent des prestations de cryptologie visant à assurer une fonction de confidentialité sont tenues de remettre aux agents autorisés dans les conditions prévues à l'article 4, sur leur demande, les conventions permettant le déchiffrement des données transformées au moyen des prestations qu'elles ont fournies. Les agents autorisés peuvent demander aux fournisseurs de prestations susmentionnés de mettre eux-mêmes en oeuvre ces conventions, sauf Si ceux-ci démontrent qu'ils ne sont pas en mesure de satisfaire à ces réquisitions.

"Le fait de ne pas déférer, dans ces conditions, aux demandes des autorités habilitées est puni de deux ans d'emprisonnement et de 30 000 euros d'amende.

"Un décret en Conseil d'Etat précise les procédures suivant lesquelles cette obligation est mise en oeuvre ainsi que les conditions dans lesquelles la prise en charge financière de cette mise en oeuvre est assurée par l'Etat. "

OBJET

L'article 11-1 nouveau de la loi n° 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des télécommunications contraint, en outre, les personnes qui fournissent des prestations de cryptologie à remettre les conventions permettant le déchiffrement des données ainsi cryptées aux autorités administratives habilitées à réaliser des interceptions dans les conditions prévues par ladite loi. Le fait de ne pas déférer à cette demande est puni d'une peine de deux ans d'emprisonnement et de 30.000 E d'amende.

PROJET DE LOI
SECURITE QUOTIDIENNE
(nouvelle lecture)

6 octobre 2001

AMENDEMENT N° 12

Présenté par

LE GOUVERNEMENT

_____

ARTICLE ADDITIONNEL APRÈS L'ARTICLE 6 TER

Apres l'article 6 ter, insérer un article additionnel ainsi rédigé:

Aprês l'article 706-70 du code de procédure pénale, il est inséré un titre XXIII ainsi rédigé:

“TITRE XXIII

“De l'utilisation de moyens de télécommunications au cours de la procédure

“ Art. 706-71.- Lorsque les nécessités de l'enquête ou de l'instruction le justifient, l'audition ou l'interrogatoire d'une personne ainsi que la confrontation entre plusieurs personnes peuvent être effectués en plusieurs points du territoire de la République se trouvant reliés par des moyens de télécommunications garantissant la confidentialité de la transmission. Il est alors dressé, dans chacun des lieux, un procès verbal des opérations qui y ont été effectuées. Ces opérations peuvent faire l'objet d'un enregistrement audiovisuel ou sonore, les dispositions du quatrième à neuvième alinéa de l’article 706 - 52 sont alors applicables.

“En cas de nécessité, résultant de l'impossibilité pour un interprète de se déplacer, l'assistance de l'interprète au cours d'une audition, d'un interrogatoire ou d'une confrontation peut également se faire par l'intermédiaire de moyens de télécommunications.

“Les dispositions du présent article sont également applicables pour l'exécution simultanée, sur un point du territoire de la République et sur un point situé à l'extérieur, de demandes d'entraide émanant des autorités judiciaires étrangères ou des actes d'entraide réalisés à l'étranger sur demande des autorités judiciaires françaises.

“Un décret en Conseil d'Etat précise, en tant que de besoin, les modalités d'application du présent article.”.

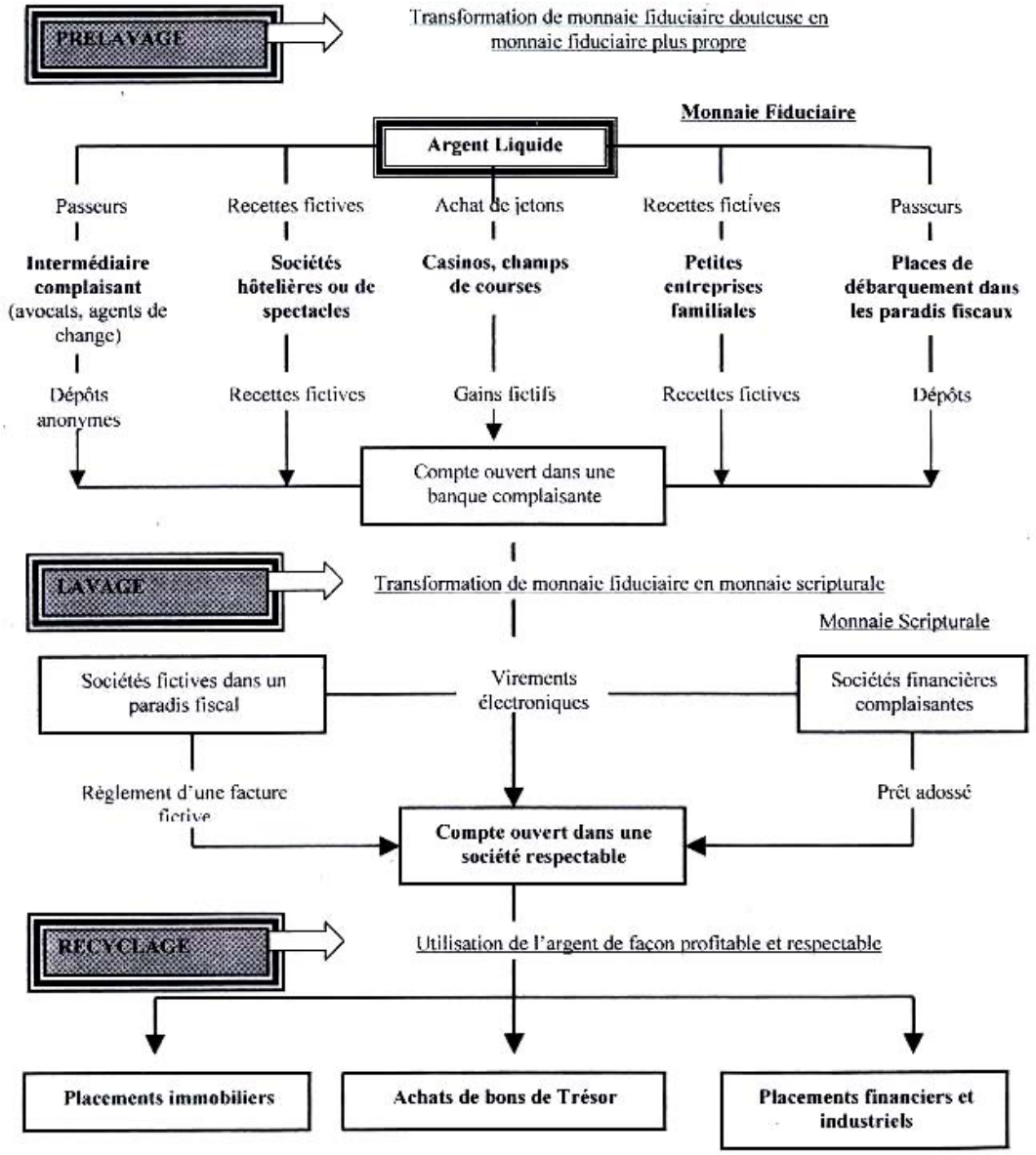
OBJET

Il parait indispensable d'autoriser l'utilisation de moyens de communication audiovisuelle au cours de la procédure pénale, qui permet dans le cadre de procédures anti-terroristes d'interroger des personnes à distance, d'assurer la célérité, la sécurité et l'efficacité des procédures et de

surmonter des obstacles procéduraux ou physiques liés au déplacement de ces personnes ou des autorités susceptibles de les entendre et constituerait le complément indispensable de l'échange d'informations entre services de lutte contre le terrorisme.

L'utilisation de ces techniques modernes de communication - qui a déjà été consacrée en 1998 par les articles L. 952-7 (Il) et L. *952-11(11)* du code de l'organisation judiciaire pour la juridiction de Saint-Pierre-et-Miquelon - est d'ailleurs préconisée par plusieurs instruments internationaux, et elle présente un intérêt tout particulier en matière d'entraide judiciaire internationale, spécialement en matière de lutte contre le terrorisme.

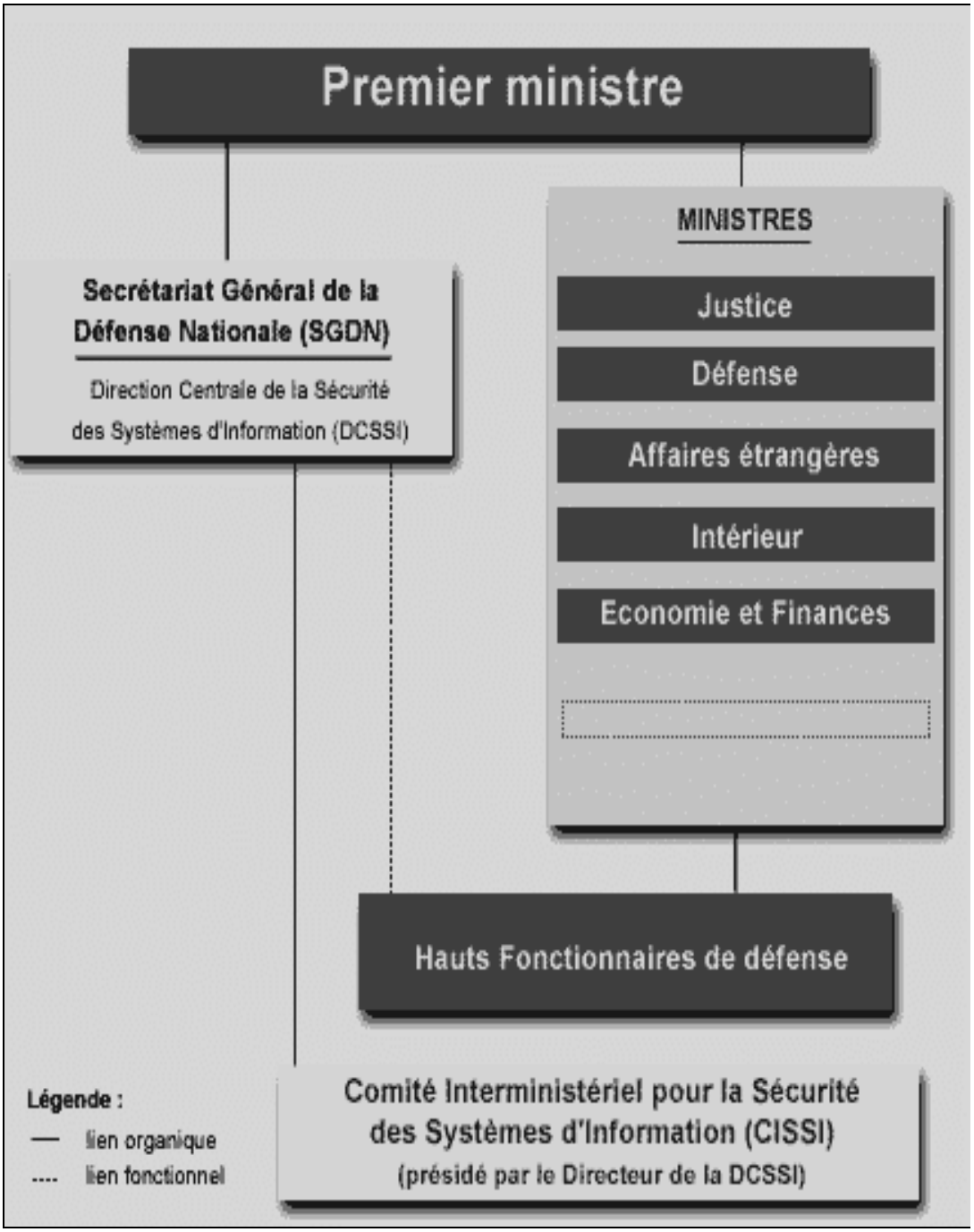
Schéma du processus du blanchiment[152]



[152] Schéma proposé par NGUYEN-VO S. et TONNET F., exposé « Internet et blanchiment d'argent », dans le cadre du DESS Droit public des NTSI, Nanterre, 2001-2002.

Direction Centrale de la Sécurité des Systèmes d'Information

dans l'organisation de la sécurité des systèmes d'information



Notions pratiques

Dans la pratique, toutes les données d'un ordinateur sont stockées dans des fichiers eux mêmes classés dans des répertoires et le tout sur un disque dur. L'utilisateur peut protéger ses fichiers par des mots de passe ou restreindre la lecture, la modification ... Dans Word et Excel, par exemple, cette option est disponible afin pour protéger des informations sensibles.

De même pour les répertoires, sur certains systèmes d'exploitation (NT, XP en particulier et particulièrement sur les environnements Linux/Unix) le propriétaire du dossier peut en limiter l'accès. Exemple : le répertoire où sont stockées toutes les factures au format numérique est en accès restreint : seul le comptable et les dirigeants de l'entreprise y ont accès. Le principal risque est l'utilisation de l'outil informatique en réseau. Ainsi dans une entreprise, un utilisateur averti peut aisément accéder (lire, modifier, effacer) au fichier d'un utilisateur apprenti. Internet amplifie ce risque dans la mesure ou le néophyte fait face à des millions d'utilisateurs plus expérimentés et potentiellement malintentionnés. C'est pourquoi, pour des échanges de données sensibles au travers du réseau on utilise des connections cryptées. Les connections du type SSL, par exemple, sont très utilisés dans les systèmes de paiement en ligne. Pour utiliser ce type de connexion (le SSL) il faut installer un certificat (carte d'identité de la machine) sur le serveur (machine sur laquelle les données sensibles sont). Quelques grandes sociétés sont connues pour fournir ce genre de services aux professionnels et aux particuliers comme Verisign, RSA, Thawthe ...

Pour prendre un exemple concret les plateformes de paiement sur Internet sont accessibles via une connexion sécurisée (https contre http d'habitude). De même, certains utilisateurs utilisent des e-mails cryptés. Pour cela ils ont installé un certificat (toujours une fiche d'identité mais cette fois au niveau utilisateur) ce certificat permet d'authentifier la provenance de données (on est certain que cet e-mail vient de l'expéditeur mentionné sur le mail...).

Les entreprises mettent en place entre leur différents établissements des VPN (Virtual Private Network) qui leur permettent de limiter l'accès aux seuls membres de l'entreprise et surtout de ne faire circuler les données qu'à travers ‘des tuyaux’ réservés à l'entreprise (utilisateurs et/ou stations) de travail.

Toutes ces données, parfois très sensibles, ne sont pas toutes protégées de la même façon.

Les grandes entreprises emploient des administrateurs réseaux qui vont superviser les ‘comptes utilisateurs’, les accès réservés, les zones sécurisées, les machines protégées, les serveurs, les accès entrants et sortants, la diffusion potentielle de virus dans le parc informatique de l'entreprise...
A l'entrée du réseau de l'entreprise une machine filtre les données et les connections : on appelle ce type de machines les ‘Firewall’.

Lorsque vous stockez vos données chez des professionnels dans des ‘coffres forts’, ces dernières seront plus à l'abri que sur l'ordinateur d'un utilisateur peu averti ou connexion non sécurisée.
Les sauvegardes peuvent se faire sur des supports matériels comme des Cd-rom ou des bandes (ces dernières permettent de stocker deux cents (200) fois ! plus de données qu'un cd-rom). Ces supports pouvant être rangés dans une armoire ou déposés dans des coffres forts.