

Citation : Eric A. Caprioli, *Anonymat et commerce électronique*, <http://www.caprioli-avocats.com>

Première publication : *Les premières journées internationales du droit du commerce électronique*, Actes du colloque de Nice des 23, 24 et 25 octobre 2000, coll. Actualités de droit de l'entreprise, dirigée par J. Raynard, Litec, 2002, p. 149 s.

Date de la mise à jour : octobre 2000

ANONYMAT ET COMMERCE ELECTRONIQUE

[Eric A. Caprioli](#)

email : contact@caprioli-avocats.com

Plan

INTRODUCTION

1) L'anonymat : une liberté fondamentale et un droit de la personnalité protégés

A) Nouvelles atteintes et nouvelles parades techniques

1) De nouveaux dangers pour les droits des personnes

2) Parades techniques d'anonymisation

B) Les protections juridiques de l'anonymat

1) Usage du pseudonyme

2) Respect de la vie privée

3) Données personnelles

4) Anonymat et autorégulation

II) L'anonymat : une liberté et un droit sous contrôle

A) La nécessaire identification des personnes : l'obligation de rendre compte

1) L'identification des personnes éditant un service de communication en ligne

2) L'identification volontaire à des fins probatoires

B) Obligations incombant aux prestataires de services de la société de l'information

1) Intermédiaires techniques

2) Prestataires de services de certification (P.S.C.)

[Notes](#)

INTRODUCTION :

L'anonymat est une notion complexe empreinte d'ambiguïté; elle se trouve au confluent de valeurs politique, économique, juridique, morale et philosophique. Les intérêts en présence divergent selon que l'on se place du point de vue de l'individu ou de celui de la société. L'actualité récente témoigne parfois de la gravité du sujet : au Royaume Uni, deux mineurs meurtriers d'un autre enfant, devant être remis en liberté, demandent à bénéficier d'une nouvelle identité de sorte que leur anonymat soit préservé.

"Garder l'anonymat" dans les relations du commerce électronique, voire de façon plus large lors de tout échange électronique sur les réseaux numériques rime avec le fait de pouvoir agir « *sous couvert de l'anonymat* ». Ainsi, l'anonymat consisterait « *en l'état de la personne ou de la chose qui est anonyme* », c'est-à-dire la personne « *dont on ignore le nom, ou qui ne fait pas connaître son nom* », ou « *dont le responsable n'a pas laissé son nom ou l'a caché* » ([1]). Une personne est anonyme lorsqu'elle « *n'a pas de nom patronymique ou qui ne porte pas de nom de personne* » ([2]). Une grande majorité des individus entend demeurer anonyme lors de leurs circumséambulations sur les réseaux numériques ([3]). L'anonymat est revendiqué pour l'ensemble des activités que l'on peut exercer : échanges de courriers électroniques, « *butinage* » sur les sites d'informations ou de commerce, actes de paiements en ligne, forums de discussion, ...

Selon une opinion (erronée) assez répandue « *sur l'Internet, l'anonymat est à peu près total* », certains en ont déduit qu'en l'absence de pression sociale – les relations étant non physiques –, cela érodait la morale ([4]).

L'anonymat s'inscrit dans le cadre des droits et des libertés fondamentaux de la personne "humaine". Les enjeux juridiques de l'anonymat résident à la fois dans le droit au respect de la vie privée (15), dans la liberté d'expression (16), telle qu'énoncée notamment à l'article 11 de la Déclaration des droits de l'homme (17), ainsi que dans la liberté de communication, version moderne de la liberté d'expression (18). Le principe du droit au respect de sa vie privée est consacré par la loi du 17 juillet 1970 (art. 9 c. civ.). Le droit au respect de l'intimité de la vie privée inclut l'anonymat. Toute atteinte à l'anonymat « doit être justifiée par une finalité explicite » (19). La recherche de cette finalité initiale ayant conduit à la levée de l'anonymat, c'est à dire à l'identification d'une personne déterminée, a permis à Messieurs Robert et Duffar de distinguer trois types d'atteintes : les secrets de la personne, la fixation et la divulgation des expressions du corps et la protection des informations nominatives (10).

Pourtant, à de multiples occasions, les activités sociales conduisent les individus à se faire reconnaître. Ainsi, lorsqu'un individu circule dans le monde physique, il est susceptible de faire l'objet de contrôle d'identité tant sur le territoire qu'aux frontières des États. Pour les besoins de la cause, l'intervention de l'État a progressivement transformé le nom en institution de police. Mais il ne faut pas omettre le fait que les personnes laissent aussi des traces de leurs passages physiques dans les mémoires d'éventuels témoins, ce qui permet l'identification visuelle dans le cadre des enquêtes judiciaires. Ainsi, l'individu est supposé connaître, même sans en avoir toujours pleinement conscience, le dévoilement de son nom et/ou de son image, partie de son intimité. En revanche, toute connexion au réseau, tout passage sur un site, toute expédition de message peuvent être enregistrés à l'insu des individus. Les données d'identification recueillies changent, la finalité diffère : la récolte de données identifiantes ne conduit pas forcément à la commission d'une infraction pénale, mais plutôt à l'abreuvement de bases de données marketing.

Si par exemple un professionnel astreint au secret en vertu de l'article 226-13 c. pén. (avocat, médecin ou assistant de service social) devait transmettre par voie électronique des données nominatives couvertes par ledit secret (consultation juridique, dossier médical, fiche de signalement, ...), toute atteinte au secret des correspondances privées sera sanctionnée pénalement (articles 226-15 et 432-9 c. pén.) (11). En outre, le professionnel concerné a le devoir d'assurer préservation de la confidentialité de ce type d'échange en utilisant des moyens de cryptologie appropriés (12). Lorsque les parties signent un acte sous seing privé, cela nécessite l'emploi de moyens de cryptologie garantissant la fiabilité du procédé de signature utilisée pour acquérir la force probante de l'écrit. La technologie de la cryptologie à clés asymétriques permet d'assurer trois fonctions essentielles : identification, intégrité et confidentialité (13).

D'après d'éminents civilistes, si l'anonymat est une liberté liée au port du nom, elle cesse dès lors qu'elle lèse l'intérêt légitime d'un tiers (14). Cette acception nous invite néanmoins à déterminer en quoi, le contenu et les frontières de l'anonymat dans le monde virtuel (sur les réseaux numériques) diffère de celui de la vie réelle. Si la problématique juridique est ancienne, en revanche, de nouvelles menaces apparaissent. Selon Mme Pousson-Petit, l'anonymat est un concept relativement récent, encore peu utilisé en France et qui est apparu en premier lieu en droit public (15). Son origine serait tirée de la "privacy" anglo-saxonne. L'anonymat se manifeste de multiples façons telles l'accouchement sous X, l'œuvre de l'esprit anonyme, les dons d'organes, de sang et de sperme (16) ou la plainte contre X. Pour certaines personnes se trouvant dans des situations particulières, c'est même le législateur qui l'impose en vue de protéger leur vie privée : adoption, assistance médicale à la procréation. En tout état de cause, le droit français place l'anonymat parmi les libertés publiques et une partie de la doctrine le considère également comme un droit fondamental (17), « le droit de s'opposer à l'investigation ou à la divulgation de son identité ou de son intimité » (18).

Ceci confère un caractère hybride à l'anonymat dès lors qu'il est en même temps une liberté publique et un droit de la personnalité. Ses sanctions juridiques revêtent des formes tant civiles que pénales. A l'instar d'autres droits de la personnalité, tels que le droit au respect de la vie privée et le droit à l'image, qui "sont plus particulièrement visés par un élément très fort de restriction : le droit public à l'information" (19), le droit à l'anonymat se trouve limité par l'obligation de rendre compte, dont l'effectivité sur les réseaux numériques passe désormais par le recours à l'obligation de fournir des données d'identification qui pèsent sur les intermédiaires techniques (20).

L'identification des personnes est inhérente à l'obligation d'avoir un nom ainsi que par le devoir de le porter, elle constitue la règle pour les actes officiels (21). Dès lors la liberté d'être anonyme doit s'entendre comme l'absence d'identification (22).

L'anonymat serait ainsi considéré comme " l'ultime rempart de la liberté et de la vie privée " (23), un nouveau combat politique pour la défense des libertés. Dans le prolongement de la pensée de M. Edelman, on peut se demander si les réseaux numériques n'engendrent pas de nouveaux dangers pour la personne ? (24). D'un autre point de vue, l'anonymat serait source d'incivisme et d'actions délictuelles, il empêcherait l'identification du débiteur ou du délinquant. Sur un autre plan, il apparaît que de nombreux sites ne comportent pas d'information sur l'identité de leur titulaire. Dans ce cas l'anonymat du site web ne permet pas aux victimes d'entamer des poursuites judiciaires. La directive européenne du 8 juin 2000 « sur le commerce électronique » impose l'obligation de faire figurer sur les sites web connectés à l'Internet des informations minimales (article 6), ainsi que celle de fournir d'autres informations avant la passation de commande (article 10) (25). Anonymat et identification constituent les deux faces d'une même pièce.

Dès lors, il conviendra de préciser dans un premier temps les contours et le contenu de la protection de l'anonymat dans le commerce électronique (I), entendu en tant que liberté fondamentale et droit de la personnalité et dans un second temps, de tracer les limites de cette liberté et de ce droit, sous contrôle (II).

I) L'anonymat : une liberté fondamentale et un droit de la personnalité protégés

L'examen des principales menaces qui pèsent sur les personnes lorsqu'elles naviguent de sites en sites (A) nous permettra de mettre en exergue les différents moyens de protection mis en place par la pratique sur le plan technique d'une part, et les protections que le droit offre aux individus, d'autre part (B).

A) Nouvelles atteintes et nouvelles parades techniques

Par définition, l'anonymat peut être passif ou actif. Dans la première hypothèse, l'objectif réside dans le désir d'éviter d'être identifié lorsqu'on dispose d'une connexion à l'Internet, c'est à dire dès lors que l'on interagit avec un ou plusieurs internautes ou que l'on va sur une page web. Le but poursuivi est le respect de la vie privée.

Dans la seconde hypothèse, le souci est sensiblement différent, car sur l'internet, les données identifiantes "ne permettent pas de retrouver la personne dans son contexte physique, mais offrent un point d'ancrage, un point d'amalgame permettant d'agréger des informations relatives à une personne." ([26]). L'individu va chercher à effacer ses propres données identifiantes ou à les omettre. Ces données sont celles relatives à l'identité civile (nom, domicile, ...), aux codes d'identification (numéro NIR, numéro SIREN pour un professionnel libéral, numéro de carte de crédit, ...), voire celles qui ont trait au physique de la personne (physiologie, morphologie, voix, données biométriques telles que les empreintes digitales, génétiques).

Face aux " multiples visages de l'anonymat actif", M. Etienne Davio procède à une classification en fonction des finalités poursuivies ; celles-ci sont au nombre de quatre, les deux premières sont exceptionnelles, la troisième s'adresse à l'autorité étatique et enfin la dernière consiste à s'exclure des modèles économiques dominants inhérents à la société de l'information :

- l'anonymat de l'auteur de certains faits juridiques régis par des textes spéciaux (accouchement sous X, adoption, ...)
- l'anonymat pour assurer la sauvegarde des intérêts des parties au contrat (prête-nom pour préserver l'identité d'un contractant paiement en espèces afin d'assurer la confidentialité du contrat) ;
- l'anonymat pour assurer la liberté d'expression ;
- l'anonymat comme rempart de la vie privée ([27]).

1) De nouveaux dangers pour les droits des personnes

Actuellement des services en ligne permettent aux internautes de retrouver leurs noms sur le réseau internet, ainsi que des quantités d'information les concernant ([28]) ; mais cette possibilité peut être utilisée par autrui. Les menaces sont nombreuses et bien réelles. L'anonymat sur l'Internet peut être recherché dans plusieurs cas : permettre l'exercice de la liberté d'expression, interdire toute atteinte à la vie privée et dans les opérations contractuelles. Pour mieux saisir les formes que prend la quête d'anonymat, il conviendra d'envisager les techniques d'identification et ses avatars, spécifiques à l'environnement numérique

a) Généralités sur les méthodes d'identification sur l'internet

Il arrive souvent que ce soit l'individu lui-même qui s'identifie volontairement en utilisant un procédé de signature numérique ou en fournissant ses coordonnées électroniques. Dans une autre optique, un pirate informatique laisse des traces de ses passages, permettant ainsi de le localiser et de l'appréhender dans le cadre de poursuites pénales.

Cependant, d'autres méthodes d'identification résultent directement des moyens de communication utilisés. L'identification ne recherche pas forcément à retrouver l'identité civile de la personne mais plutôt à suivre ses agissements, à dresser son profil de consommation, à le joindre ultérieurement à son adresse pour des offres promotionnelles adaptées à son profil ([29]). Ces éléments d'identification peuvent être couplés à d'autre figurant dans des bases de données et permettre ainsi une identification de la personne physique. Sans doute, est-il permis de penser que ces eldorados de la consommation ont eu quelque influence sur le développement de la nouvelle économie ?

L'exemple suivant illustre la complexité de la problématique : une personne avait utilisé l'ordinateur et l'accès internet mis à disposition des administrés en libre accès par une commune dans les locaux de sa bibliothèque. L'utilisateur qui ne s'était pas fait connaître avait acheté des biens en ligne avec une carte de crédit volée. La justice saisie par l'e-commerçant avait localisé l'ordinateur en cause sans problème, mais cela ne servit à rien dans la mesure où de nombreuses personnes pouvaient y accéder. Aucun registre d'utilisation avec l'heure et le nom de la personne n'était tenu par le personnel communal. C'est grâce à l'adresse physique de livraison des biens achetés que l'interpellation contre le délinquant a été possible ([30]).

b) Les adresses IP (Internet Protocol)

Avec le protocole TCP/IP (Transmission Control Protocol over Internet Protocol) ([31]) chaque ordinateur qui se connecte au réseau est identifié. Ces adresses sont toujours communiquées à l'occasion des échanges de courriers électroniques et lors des consultations de sites Web. L'adresse autorise l'identification d'un objet (une machine) et du lieu d'entrée sur le réseau ([32]). A ce stade, on doit distinguer les adresses IP temporaires et les adresses IP permanentes. Ces dernières sont attribuées durablement à un ordinateur donné, alors que les premières sont attribuées à l'internaute pour la durée de sa connexion par son fournisseur d'accès. A chaque connexion au réseau, l'adresse change. La seule possibilité de retrouver un délinquant réside dans la fourniture de l'identité civile de la personne titulaire de l'adresse IP par le fournisseur d'accès. Or, comme nous l'avons vu ci-dessus, la seule adresse IP ne suffit pas pour retrouver la personne physique à qui l'acte ou le fait juridiques

est imputable. Ces adresses brutes ne constituent pas, à notre sens, des données personnelles en tant que telles. Et même s'il existe des risques d'atteinte à la vie privée, en aucun cas les adresses IP ne permettent de porter atteinte au caractère confidentiel des messages. Nous examinerons dans la seconde partie de l'étude les récentes dispositions législatives intervenues en la matière.

c) Les adresses de courrier électronique

Fréquemment le nom de la personne physique (et le prénom) ou de l'organisation figure à gauche de l'arobace "@" ([33]), suivi de l'adresse de la machine du fournisseur d'accès et de son pays d'origine ou de son activité (ex : caprioli@dial-up.com). En telles hypothèses, les adresses permettent d'identifier et de suivre les personnes dans le temps. En effet, c'est à la personne à qui on associe l'adresse que l'on va attribuer les messages reçus d'elle et à qui l'on va répondre, voire que l'on va solliciter avec des courriers publicitaires. A ce titre, les adresses de courrier électronique sont protégées par loi « *Informatique, fichiers et liberté* », ce qui n'exclut pas le recours aux infractions pénales pour réprimer les diverses techniques de captation d'adresses ([34]). Si l'adresse se compose de chiffres ou codes, la seule possibilité de retrouver l'identité consiste à s'adresser au fournisseur d'accès.

Certains évoquent un « *commerce d'identités électroniques* » au sujet des adresses de courriers électroniques ([35]). L'attribution de ces adresses s'effectue pratiquement sans aucun contrôle, contrairement par exemple au dépôt d'un nom de domaine en « .fr ». De la sorte, elles peuvent faire l'objet de manipulations et conduire à toutes sortes de trafic ([36]).

d) Le nom de domaine

La question des noms de domaine comporte plusieurs dimensions juridiques dont l'une a trait au droit de propriété intellectuelle en ce qu'il est un signe distinctif légalement protégé quoique ne pouvant être assimilé à l'un des signes distinctifs reconnus en droit positif ([37]). L'autre dimension qui retient l'attention du juriste est celle du domicile ou du siège social virtuel ([38]). Le nom de domaine est supposé donner une image aussi proche que possible de l'activité du site concerné. Pourtant, pour peu que l'on interroge les organismes de gestion des noms de domaine (AFNIC, NSI, ...), il est possible de connaître le nom du titulaire, ceux des contacts administratif et technique, ... Par ce moyen, on peut facilement obtenir l'identité et l'adresse électronique du responsable d'un site web. On peut voir dans cet état de fait une nouvelle atteinte à l'anonymat.

e) Les cookies

Un cookie est une sorte de témoin utilisé dans le protocole Http que certains qualifient de mouchard. Ce petit fichier est utilisé dans les environnements client-serveur et permet d'obtenir des informations sur le client lors d'une session. A partir du moment où l'on se connecte sur un serveur celui-ci peut enregistrer des informations sur l'ordinateur client. Ces informations seront relues et exploitées au moment d'une nouvelle connexion. Ainsi le cookie peut déclencher des actions sur le site : modification des pages, des bandeaux publicitaires, de l'ordre de présentation des hyperliens, ouverture d'une fenêtre publicitaire, etc. Les cookies sont la clé de voûte du e-marketing et du commerce électronique. Toutefois, les navigateurs permettent d'accepter ou de refuser les cookies avec plus ou moins de facilité pour l'utilisateur. La fédération des professionnels de la vente à distance a décidé que ses adhérents devaient demander aux consommateurs s'ils acceptent ou non le cookie (opt-in et opt-out) ([39]).

f) Monnaie et porte-monnaie électroniques

Alors que la monnaie a revêtu des formes fort diverses au cours des siècles : « *troupeaux, coquillages, lingots, billets* » ([40]), d'autres moyens de paiements sont utilisés (chèques, lettres de change, cartes bancaires). On peut sans peine distinguer les moyens qui préservent l'anonymat de ceux qui ne le préservent pas. La monnaie fiduciaire fait partie de la première catégorie. Le droit moderne, en imposant l'obligation de payer par chèque (ou par carte) a introduit une importante restriction au principe de l'anonymat ([41]). Le pouvoir réglementaire interdit aux commerçants, d'accepter des règlements en espèces au-delà d'un montant déterminé, progressivement de plus en plus faible. A ce titre, il convient de souligner que la loi de finances pour 2001 impose aux particuliers non commerçants de payer par carte de crédit, chèque ou virement toute acquisition d'un bien ou d'un service supérieur à un montant de 20.000 francs TTC ([42]). D'ailleurs, les commerçants ne connaissent-ils pas déjà des restrictions légales quant au paiement des salaires (10.000 francs) ou de certaines factures au-delà d'un certain seuil ([43]).

Aux termes de la directive du 18 septembre 2000 concernant l'accès à l'activité des établissements de monnaie électronique et son exercice ainsi que la surveillance prudentielle de ces établissements ([44]), la monnaie électronique est une valeur monétaire qui est stockée sur un support électronique (carte à puce ou disque dur), émise contre remise de fonds d'un montant dont la valeur n'est pas inférieure à la valeur monétaire émise et acceptée comme moyen de paiement par les entreprises autres que l'institution émettrice ([45]). De son côté, le porte-monnaie électronique consiste à conserver de la « *monnaie* », soit sur support physique (carte ou autres), soit sur un système informatique centralisé. C'est, à notre connaissance, la seule technique de paiement en ligne qui préserve l'anonymat, contrairement aux divers moyens de paiement à l'aide de la carte bancaire ou autres méthodes en ligne ([46]) qui laissent des traces, à tout le moins auprès des établissements de crédit. Les traces de paiement demeurent indélébiles ; elles permettent de surveiller non seulement la nature et le montant des transactions, mais également les déplacements de l'individu visé lors de chaque transaction.

2) Parades techniques d'anonymisation

Plusieurs techniques de protection de l'anonymat ou d'anonymisation existent ([\[47\]](#)), nous nous pencherons rapidement sur trois exemples afin d'illustrer notre propos : les solutions de protection de l'anonymat, les remailers et les sites d'anonymisation.

S'agissant au premier chef **des solutions de protection de l'anonymat**, il convient de remarquer qu'il n'y a encore que très peu de produits, actuellement disponibles sur le marché, qui offrent à la fois une solution complète et véritablement efficace. L'objectif est de traiter la problématique des cookies ainsi que la récupération des adresses IP. Par exemple, la solution « *Lucent Personalized Wew Assistant* » (« *LPWA* ») permet de relayer tout le trafic de l'utilisateur de sorte que la seule adresse qui soit enregistrée soit « *lpwa.com* » ; les serveurs web n'ont ni la possibilité d'enregistrer des cookies sur le disque, ni celle de récupérer l'adresse IP de l'utilisateur ([\[48\]](#)).

Le travail des **remailers** consiste à réaliser la réexpédition anonyme des messages. Ils réceptionnent les messages d'internaute, puis ils les réexpédient vers le destinataire, mais en ayant préalablement supprimé toutes les informations permettant l'identification de l'expéditeur (à savoir, le champ sur le message contenant l'adresse électronique, l'adresse IP de l'auteur du message), ainsi que les sites visités antérieurement.

Enfin, en ce qui concerne les **sites d'anonymisation**, des organisations proposent de servir d'écran aux internautes lors de leurs navigations sur l'internet. Ils utilisent des serveurs proxy de manière à prévenir toute identification qui pourraient intervenir grâce aux cookies et à l'aide de l'adresse IP ([\[49\]](#)). De tels services d'anonymisation se développent que ce soit au cours de la navigation ou lors du paiement en ligne ([\[50\]](#)).

Ces techniques ne sont pas pour l'instant la panacée universelle, c'est pourquoi, loin d'être négligeable, la protection juridique est une nécessité incontournable. Les outils juridiques existent.

B) Les protections juridiques de l'anonymat

La principale protection des attributs de la personne physique se trouve à l'article 1382 c. civ., donc dans l'action en dommages-intérêt ayant pour fondement juridique la faute de celui qui aurait porté atteinte aux droits de la personnalité, aux libertés individuelles, au respect de la vie privée (et à l'égalité civile) ([\[51\]](#)). Alors que l'usage de pseudonyme incarne l'exercice d'une liberté publique sous réserve de respecter certaines conditions (1), la protection de l'anonymat prend corps dans le droit au respect de la vie privée et dans le droit des données à caractère personnel (2) et (3).

Ces aspects nous permettront de déterminer comment la protection juridique de l'anonymat est assurée.

1) Usage du pseudonyme ([\[52\]](#))

Parmi les institutions humaines, le nom est sans doute la plus générale et la plus répandue. S'il sert à individualiser des personnes physiques, il assure deux fonctions d'identification : sociale et individuelle. Dominé par l'usage sous l'ancien régime, la révolution place le nom sous l'emprise de la loi, « *mais cela n'empêchera ni les surnoms, ni les sobriquets ni les pseudonymes de continuer leur carrière même s'ils sont un peu gênés par la législation existante.* » ([\[53\]](#)). Le pseudonyme ne se confond pas avec le surnom, ou sobriquet, qui est "le nom d'emprunt donné à une personne par les autres. Le pseudonyme est un nom d'emprunt qu'une personne se donne elle-même." ([\[54\]](#)). Parfois fantaisistes ou d'emprunts, nombreux sont les hommes célèbres à les avoir utilisés : Molière, Voltaire, Le douanier Rousseau, Montand, Johnny Hallyday, Eddy Barclays. Par ailleurs, même si le pseudonyme ne possède pas de valeur juridique en tant que telle, il bénéficie des mêmes protections que le nom contre toute usurpation par un tiers ([\[55\]](#)) ou utilisation comme marque ([\[56\]](#)). Le véritable nom de son titulaire fait aussi l'objet de protection contre la divulgation par un tiers qui en a connaissance ([\[57\]](#)). Il peut être cédé, mais ne figure pas sur les pièces d'identité officielles.

Selon le Doyen Cornu, dès lors que le devoir de porter un nom est déterminé par la loi pénale (faux et usage de faux, dont l'usage d'un faux nom), il n'existe pas d'obligation de porter son nom ([\[58\]](#)). En dehors des délits prévus par la loi, cette liberté "résiduelle" laisse libres les individus d'utiliser d'un faux nom et légitime l'usage d'un pseudonyme ([\[59\]](#)). A la différence de son utilisation traditionnelle, où le pseudonyme d'une personne consiste à masquer au public sa personnalité par l'usage du nom figurant sur l'œuvre littéraire, philosophiques ou artistiques ([\[60\]](#)), sur les réseaux l'objectif poursuivi est plus beaucoup large, il peut, selon le choix de chacun, viser aussi bien l'anonymat pour toutes activités socio-informatique que pour certaines d'entre elles uniquement : les visites de sites commerciaux (y compris ceux à caractère pornographique ou les forums de discussion) où l'on ne veut pas être tracé, profilé ou repéré. En ce sens, on peut estimer que l'usage d'un pseudonyme constitue une marque de l'expression du droit à l'anonymat et qu'à ce titre il est protégé en tant que liberté. Mais l'expression de ce droit, notamment en signant un acte juridique, ne doit pas faire subir de préjudice aux tiers comme par exemple à l'occasion de l'usage d'un faux nom à des fins d'escroquerie (article 313-1 c. pén.). Cette infraction pourrait s'appuyer sur l'utilisation d'un pseudonyme. Toutefois, nous verrons plus avant que même lorsque le pseudonyme est utilisé dans un certificat électronique de signature, cette liberté s'arrête à l'orée de l'illicite, des infractions spécifiées par le législateur. Le pseudonyme pourrait également être protégé en tant que nom de domaine ou en tant qu'adresse électronique et servir à des fins malhonnêtes.

En droit français, l'utilisation du pseudonyme sur les réseaux (comme d'ailleurs dans la vie courante) est néanmoins suspendue au respect de certaines conditions :

- il doit être utilisé uniquement dans des activités déterminées et licites, il ne peut donc pas présenter un caractère général ;
- il ne doit pas servir à tourner des prohibitions légales ;
- son usage ne doit pas être interdit par certaines professions réglementées (médecin) ;
- il ne doit pas figurer sur un acte authentique ou un document administratif ([61]).

Le droit à l'anonymat et l'usage d'un pseudonyme sont indissociables sur les réseaux à tel point qu'ils procèdent tout deux de la volonté des individus.

2) Respect de la vie privée

Le respect de la vie privée est un principe constitutionnalisé par le Conseil constitutionnel ([62]). Si le concept de vie privée n'est pas précisément déterminé, il est au moins certain que l'état des personnes, l'adresse, le domicile, la santé, la religion, font partie des grands domaines de la vie privée ([63]). Leur protection résulte de l'article 9 c. civ. Pourtant, « *l'informatique aux fabuleux bienfaits comporte, en revers, une aptitude effrayante : la mémoire totale, instantanée. A la fois par la minutie, l'immensité, la fréquence des informations recensées sur la vie quotidienne, donc largement privée ; par une capacité sans limites de conservation de ces données, cela sous un volume de plus en plus restreint, qui permet le transfert instantané de telles informations ; par une aptitude de tri à la vitesse de la lumière, d'où s'ensuit la facilité des rapprochements et recoupements les plus inattendus, mais d'autant plus révélateurs.* » ([64]).

La protection de la vie privée s'entend non seulement de la réparation des préjudices subis par la personne dont la vie privée a été atteinte, mais également de mesures particulières dont celles de faire cesser le trouble par tous moyens que le juge jugera nécessaires de prononcer (telles que la mise sous séquestre ou la saisie). Au demeurant, s'il y a urgence, le juge pourra se prononcer en référé (ce qui, en pratique, est très fréquent). Notons qu'en application de l'article 46 NCPC, la juridiction compétente pour connaître des atteintes à la vie privée sera celle où le dommage sera fait, reçu ou perçu. Par là même, le système juridique français offre une procédure d'application particulièrement large, dès lors que les éléments constitutifs de l'atteinte peuvent être réceptionnés sur le territoire de la République, les juridictions françaises seront compétentes. Or, par nature, toutes données (informations, photos, documents) circulant sur le réseau sont recevables en France. Selon la volonté des personnes, l'anonymat peut constituer un élément fondamental de leur vie privée. Ne pas faire connaître son adresse, son état de santé, ses idées religieuses peut entrer dans le champ de protection de la vie privée des personnes. A titre d'exemple, les sites médicaux qui fleurissent sur l'internet devront particulièrement se soucier de cet aspect, en sus du secret professionnel auquel les praticiens sont astreints. En effet, la confidentialité des informations relatives à l'identification mais également au traitement et à l'état de santé diagnostiqué du patient internaute devra être garantie. La protection de son anonymat est intimement liée à la préservation de sa vie privée. Mais les contours de la notion de vie privée sur l'Internet ne sont pas toujours faciles à saisir, à l'instar de ce qui existe dans le monde matériel. Ainsi, alors que les courriers électroniques personnels et individuels constituent des correspondances privées, qu'en est-il des forums de discussions ? Ces lieux d'échanges d'avis, d'opinions, de réflexion sur des sujets très divers pourraient-ils être assimilés à des lieux publics de discussion ? Si pour participer, l'internaute doit s'identifier (ce qui est de plus en plus fréquemment exigé de la part des instigateurs de ce type d'activités afin de pouvoir écarter leur responsabilité en cas de propos diffamatoires tenus par les participants au forum), les précisions portées ne pourraient-elles pas être assimilées à une violation de la vie privée des personnes ? Le système des web cams qui, sauf volonté expresse des personnes filmées ([65]), pourrait conduire, à terme, à nier la vie privée des personnes selon l'utilisation pratiquée et porter ainsi atteinte à leur droit à l'anonymat.

3) Données personnelles

L'article 4 de la loi n°78-17 du 6 janvier 1978 définit les données nominatives comme étant celles «qui permettent « *sous quelque forme que ce soit, directement ou non, l'identification des personnes physiques* » ([66]). De telles données permettent non seulement l'identification de la personne le cas échéant, mais peuvent également renseigner sur des éléments plus intimes (âge, situation familiale, activité professionnelle, revenus, goûts musicaux, ...). La collecte de ces données et leur traitement constituent un atout majeur pour les commerçants mais également pour certaines administrations. Ainsi, par exemple, la Direction générale des impôts avait décidé d'utiliser le numéro d'identification attribué par la sécurité sociale qui constitue une donnée à caractère personnel ([67]). Du point de vue du commerce ou plus exactement du marketing, les données personnelles permettent un ciblage de plus en plus tenu des consommateurs. Avec les technologies de l'information, les moyens de collecter les données personnelles sont décuplés. Mais ces données représentent une véritable transparence des individus. Aussi, selon les finalités et l'utilisation qui en est faite, ces données peuvent constituer la négation de l'anonymat sous sa forme la plus absolue. Une nuance mérite d'être d'ores et déjà apportée au regard de l'anonymat, selon une étude, la majorité des internautes interrogés ont révélé ne pas donner des renseignements exacts lorsque les données à caractère personnel leur étaient demandées. La directive européenne du 24 octobre 1995, non encore transposée en droit interne, a pour vocation d'harmoniser le régime de protection des données personnelles dans les États membres ([68]).

La collecte et le traitement des données à caractère personnel doivent faire l'objet d'une déclaration auprès de l'autorité compétente, soit en France, la C.N.I.L. (Commission Nationale de l'Information et des Libertés). De plus, les instigateurs du traitement doivent informer les personnes concernées par les données à

caractère personnel dudit traitement. Au demeurant la finalité du traitement doit être précisée et respectée (le détournement de finalité du traitement déclaré étant pénalement sanctionné : art. 226-21 c. pénal). Le contenu des demandes relatives aux données doit en outre être proportionnel à la finalité déclarée (par exemple un formulaire établi par un commerçant de chaussures qui demanderait le nombre de pièces du logement du consommateur ne serait pas justifié). De plus, et c'est là l'un des critères essentiels de la protection des données à caractère personnel, le traitement doit se faire de façon loyale. Ainsi, le collecteur de données doit veiller à ne pas les collecter par un moyen frauduleux, déloyal ou illicite et à ne pas procéder à leur traitement malgré l'opposition légitime du consommateur. A défaut, le commerçant concerné encourt des sanctions pénales (art. 226-18 c. pénal). La Chambre de Commerce Internationale insiste également sur la loyauté en la matière au moyen de charte. Enfin, dans le cadre des données personnelles, l'individu dispose d'un droit de rectification. Il doit également être nécessairement informé de la cession à un tiers des données le concernant; étant noté que lorsqu'il s'agit d'une cession à des tiers au sein de l'Union européenne (art. 11 de la directive), le cessionnaire doit fournir à la personne concernée l'identité du responsable du traitement, les finalités du traitement, les catégories de données concernées, les destinataires ou catégories de destinataires, l'informer de son droit d'accès et de rectification des données et sa faculté de s'opposer à la cession envisagée. S'il s'agit d'un transfert ou d'une cession vers un pays tiers hors Union européenne (art. 25 de la directive), les données à caractère personnel ne peuvent être cédées que si le pays destinataire offre un niveau de protection adéquat en fonction de la nature des données, de la finalité et de la durée du traitement notamment. Sur ce point, un accord important est intervenu entre l'Union européenne et les États Unis ([69]). Il a pour objet de permettre le transfert de données à caractère personnel de sociétés européennes vers des sociétés américaines (dont les filiales vers les sociétés mères) dans la mesure où le gouvernement américain s'est engagé à ce que le niveau de protection des données soit « équivalent » à celui posé par la directive. En ce domaine, la réglementation est donc venue empiéter sur le terrain de l'autorégulation américaine qui jusqu'alors régnait à l'égard des données à caractère personnel.

4) Anonymat et autorégulation

Le phénomène de l'autorégulation prend en compte les questions de vie privée et d'anonymat. Les codes et les chartes de bonne conduite ou de déontologie constituent une manifestation éclatante de la prise de conscience chez les acteurs de l'Internet. L'article 27 de la directive de 1995 consacre ce procédé de régulation, d'origine anglo-saxonne, au moyen des codes de conduite quelle que soit leur origine (par exemple nationale ou communautaire) ([70]).

Si l'on se penche par exemple sur l'un des premiers textes au plan national - la proposition de charte de l'Internet, document issue des travaux de la Commission présidée par M. Antoine Beausant et remis le 5 mars 1997 au Ministre délégué à La Poste, aux télécommunications et à l'espace -, on peut constater que son chapitre VIII ("Libertés et droits fondamentaux") contenait un article 3 disposant :

« Sur l'Internet, les utilisateurs et les personnes physiques **ont le droit de préserver**, vis-à-vis des autres utilisateurs, **l'anonymat protégeant leur vie privée**.

Cet anonymat pourra être assuré par l'utilisateur de services de relais d'anonymat tant pour le courrier électronique et la Mise à disposition de contenu que pour l'accès à des contenus.

Ces services doivent assurer et conserver les moyens de contacter les personnes qui y recourent sur la base des adresses électroniques anonymes.

Les codes, dates et heures d'accès à l'Internet peuvent toutefois faire l'objet d'une sauvegarde par le Fournisseur d'accès afin de permettre la protection des Utilisateurs du réseau contre les intrusions et la préservation de la preuve.

Le traitement automatisé d'informations nominatives par les Acteurs de l'Internet sera soumis dans tous les cas au strict respect des obligations prévues par les textes applicables (principes de loyauté et de transparence, de respect des finalités, de sécurité et de respect des droits d'accès, d'opposition et de rectification), y compris à l'occasion de l'utilisation des cookies ou de procédés similaires.

A cet effet, chaque Acteur permettra aux Utilisateurs, dans le strict cadre légal, de connaître la nature des informations collectées par l'Acteur concerné à partir de l'ordinateur de ces derniers.» ([71])

Depuis, les choses ont évolué dans un sens positif, l'information sur le sujet et la transparence des procédures sont devenues des réalités. Certains fournisseurs de services n'hésitent pas à mentionner sur leur site : « *Votre inscription effectuée, vous n'êtes plus un utilisateur anonyme pour nous, (...) et pouvez profiter pleinement des nombreux services proposés par nous.* » et nous collectons « *des adresses IP lors de votre inscription permettant en cas d'abus de répondre aux informations des autorités légales.* » ([72]). Plus largement, afin d'assurer la confiance dans le commerce électronique (et sans doute afin de rassurer leurs clients), de grands acteurs mondiaux de l'Internet mettent en œuvre des politiques de vie privée (« *privacy policy* ») ou des chartes de la confiance sur l'Internet, aux termes desquelles, ils s'engagent à respecter les droits et libertés des personnes, spécialement leur vie privée ([73]).

Les chartes, telles celle de la Commission Beausant, préfiguraient le régime qui est actuellement en train de se dessiner en matière d'anonymat sur les réseaux numériques : une liberté et un droit sous contrôle !

II) L'anonymat : une liberté et un droit sous contrôle

Toute personne ne peut se cacher derrière l'anonymat pour enfreindre la loi ou violer les droits d'autrui (diffamation, atteinte à l'honneur ou au droit à l'image, diffusion et consultation d'images à caractère pédophile, propagation d'idées ou de propos à caractère racistes ou antisémites, négationnistes, ...).

En matière pénale, la charge de la preuve incombe à la partie poursuivante (le Ministère public) en vertu du principe de la présomption d'innocence. Le Ministère public doit "établir tous les éléments constitutifs de l'infraction et l'absence de tous les éléments susceptibles de la faire disparaître" (174). S'agissant des moyens de preuve, le principe est celui de la liberté dans l'établissement de la preuve (175). Aux termes de l'article 427, al. 1 C.P.P. "Hors les cas où la loi en dispose autrement, les infractions peuvent être établies par tous moyens de preuve et le juge décide d'après son intime conviction". Tous les types de preuve sont recevables : témoignages, constatations matérielles, indices, présomptions...

Dans le cadre du projet de la Convention du Conseil de l'Europe sur la cybercriminalité (176), son préambule énonce qu'elle doit "permettre une lutte efficace contre ces infractions pénales, en facilitant la détection, l'investigation et la poursuite, tant au plan national qu'au niveau international, (...), tout en garantissant un équilibre adéquat entre les intérêts de l'action répressive et le respect des droits fondamentaux." Atteindre un tel équilibre n'est pas aisé, mais cela impose de tenter de tracer les modalités de l'action pénale.

En conséquence, sur les réseaux numériques, le droit pénal se heurte aux trois contraintes suivantes :

- l'anonymat des personnes qu'il faut impérativement localiser et identifier pour être en droit d'entamer les poursuites ;
- les informations numériques sont volatiles et par conséquent, elles sont modifiables et supprimables à volonté dans des délais records alors que les services de police doivent préserver les éléments de preuve et s'appuyer sur des données de connexion afin de caractériser l'infraction ;
- les actes illicites sur les réseaux ont une nature internationale ce qui rend plus difficile l'efficacité de leur répression essentiellement fondée sur le territoire.

Ainsi précisé, les contraintes juridiques impliquent que la conservation des données pèse essentiellement sur les opérateurs de télécommunications et sur les fournisseurs de services de la société de l'information. Leur collaboration constitue une nécessité cruciale pour établir l'identité des délinquants informatiques et la preuve de leurs délits.

L'article 16 du projet de convention dispose :

- « 1- Chaque partie adopte les mesures législatives et autres qui se révèlent nécessaires pour permettre à ses autorités compétentes d'ordonner ou d'obtenir d'une autre façon, en relation avec une affaire pénale particulière, la conservation rapide de données stockées au moyen d'un système informatique, notamment lorsqu'il y a des raisons de penser que celles-ci sont soumises à une période de conservation limitée ou sont, à d'autres titres, particulièrement sensibles aux risques de perte ou de modification.
- 2- Lorsqu'une partie applique le § 1 ci-dessus en enjoignant une personne de conserver des données stockées spécifiées se trouvant en la possession ou sous le contrôle de celle-ci, ladite Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger cette personne à conserver et protéger l'intégrité de ces données pendant la durée appropriée, afin de permettre aux autorités compétentes d'obtenir leur divulgation.
- 3- Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger le gardien des données ou autre personne chargée de conserver celles-ci à garder le secret sur la mise en œuvre desdites procédures pendant une durée prévue par son droit interne.
- 4- Les prérogatives et les procédures visées par le présent article sont subordonnées aux conditions et garanties prévues par le droit interne. » (177)

Pour mettre en œuvre les procédures visées à l'article précédent, l'article 17, intitulé « Conservation rapide et divulgation rapide de données relatives au trafic » (178) prévoit que « chaque partie adopte les mesures législatives et autres qui se révèlent nécessaires pour :

- a. veiller à la conservation rapide de ces données relatives au trafic, indépendamment de la question de savoir si un seul ou plusieurs fournisseurs de service ont participé à la transmission de cette communication ; et
- b. assurer la divulgation rapide à l'autorité compétente de la Partie, ou à une personne désignée par cette autorité, qu'une quantité suffisante de données relatives au trafic, aux fins d'identification des fournisseurs de service et de la voie par laquelle la communication a été transmise. »

À la vérité, les États se servent de la technique pour parvenir à leurs fins en faisant peser sur les prestataires de services de la société de l'information des obligations juridiques permettant l'identification des personnes et la collectes de traces baptisées pour les besoins de la cause « données relatives au trafic » (179). Sans ces données « d'identification », de nombreuses poursuites judiciaires risquent de s'avérer stériles.

Des limites à l'exercice du droit à l'anonymat existent, elles touchent non seulement les personnes elles-mêmes à l'instar de ce qui existe dans le droit commun (A), mais aussi les prestataires de services de la société de l'information (B). Au moyen de divers obligations relatives à l'identification, on constatera que l'anonymat est placé sous contrôle. Dès lors que l'identité sur les réseaux adopte de nouveaux contours, il n'est pas étonnant que les moyens d'identification changent. Dès lors que l'identité sur les réseaux adopte de nouveaux contours, il n'est pas étonnant que les moyens d'identification changent (180).

A) La nécessaire identification des personnes : l'obligation de rendre compte

Le droit privé s'intéresse exceptionnellement à l'identité des personnes physiques comme le souligne M. Alain Bernard, « *les juristes préfèrent parler d'identification, entendue comme "action d'identifier" ou comme "résultat de cette action". Cette attitude signale déjà que le droit s'intéresse moins à la personne qu'à son réseau de relation et montre à la fois l'intérêt mais aussi les limites du sujet* » ([81]). Mais le droit ne se conforme-t-il pas à l'anthropologie sociale « (...) *une identité grossière, immédiate, une identité "d e surface" doit laisser la place à une quête des structures profondes qui façonnent l'identité dans son aspect relationnel : la question de l'Autre apparaît comme constitutive de l'identité.* » ([82]). C'est sans doute par rapport à cet Autre que se fonde l'obligation d'identification de la personne prise en tant que telle, ainsi que dans ses relations avec les fournisseurs de services de la société de l'information.

1) L'identification des personnes éditant un service de communication en ligne

La simple lecture de l'article 43-10 tiré de la loi du 1^{er} août 2000, nous conduit à distinguer les personnes qui exercent l'activité d'édition d'un service de communication en ligne à titre professionnel de celles qui l'exercent à titre non professionnel. En effet, l'article 43-10 dispose :

- « I/ *Les personnes dont l'activité est d'éditer un service de communication en ligne autre que de correspondance privée tiennent à la disposition du public :*
- *s'il s'agit de personnes physiques, leurs nom, prénom et domicile ;*
 - *s'il s'agit de personnes morales, leur dénomination ou leur raison sociale et leur siège social ;*
 - *le nom du directeur ou du codirecteur de la publication et, le cas échéant, celui du responsable de la rédaction au sens de l'article 93-2 de la loi n°82-652 du 29 juillet 1982 sur la communication audiovisuelle ;*
 - *le nom, la dénomination ou la raison sociale et l'adresse du prestataire mentionné à l'article 43-8.*
- II/ - *Les personnes éditant à titre non professionnel un service de communication en ligne autre que de correspondance privée peuvent ne tenir à la disposition du public, pour préserver leur anonymat que le nom, la dénomination ou la raison sociale et l'adresse du prestataire mentionné à l'article 43-8, sous réserve de lui avoir communiqué les éléments d'identification personnels prévus au I."*

Au regard de la formulation adoptée, on remarquera que si le droit à l'anonymat est expressément consacré par la loi, il n'en demeure pas moins qu'il est d'une part, strictement réservé aux personnes qui éditent des contenus à titre privé et d'autre part, qu'il peut s'exercer sous réserve qu'elles aient communiqué leurs éléments d'identification personnels à leur prestataire de service d'hébergement ([83]).

2) L'identification volontaire à des fins probatoires

Une personne qui entend conclure un acte juridique sous forme électronique doit impérativement s'identifier si elle entend disposer d'une preuve parfaite. Car, outre la large définition donnée à l'écrit à l'article 1316- c. civ. « *La preuve littérale ou preuve par écrit résulte d'une suite de lettres, de caractères, de chiffres ou de tout autres signes ou symboles dotés d'une signification intelligible, quels que soient leur support et leurs modalités de transmission.*», l'article 1316-1 énonce : "*l'écrit sous forme électronique est admis en preuve au même titre que l'écrit sur support papier, sous réserve que puisse être dûment identifié la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité"* ([84]). L'identification répond à un souci de sécurité juridique, il faut être certain de l'identité de la personne qui s'est engagée ([85]) ou de celle qui s'est libérée de son obligation au moyen d'un paiement. De plus, aux termes de l'article 1316-4 al. 1 c. civ. « *la signature nécessaire à la perfection d'un acte juridique identifie celui qui l'appose...* ». L'identification des personnes est une donnée incontournable du commerce juridique.

B) Obligations incombant aux prestataires de services de la société de l'information

Nous limiterons volontairement nos développements aux prestataires de services de la société de l'information, étant précisé que les opérateurs de télécommunications (téléphones fixes et mobiles) sont également assujettis à des obligations de ce type notamment lorsque l'Officier de police judiciaire ou le Juge d'instruction fait une requête auprès d'un opérateur de téléphonie mobiles afin d'obtenir des informations relatives aux appels.

Nous examinerons successivement les obligations légales qui incombent aux intermédiaires techniques (1) et aux prestataires de services de certification (2).

1) Intermédiaires techniques

Lors de plusieurs affaires récemment portées devant les tribunaux, les fournisseurs d'hébergement ont vu leur responsabilité engagée du fait des contenus illicites qu'ils hébergeaient ([86]).

La directive européenne du 8 juin 2000 sur le commerce électronique définit en ses articles 12 à 15 les conditions de mise en œuvre de la responsabilité des intermédiaires techniques (fournisseurs d'accès, d'hébergement et de services de stockage temporaire) ([87]). A titre d'illustration, la loi du Luxembourg du 14 août 2000 relative au commerce électronique dispose à l'article 63 :

"(1) Pour la fourniture des services visés aux articles 60 à 62, les prestataires ne sont pas tenus d'une obligation générale de surveiller les informations qu'ils transmettent ou stockent, ni d'une obligation générale de rechercher des faits ou circonstances indiquant des activités illicites.

(2) Pour la fourniture des services visés à l'article 62, les prestataires (d'hébergement) sont toutefois tenus à une obligation de contrôle spécifique afin de détecter de possibles infractions aux articles 383 al. 2 et 457 -1 du Code pénal.

(3) Les paragraphes 1 et 2 du présent article sont sans préjudice de toute activité de surveillance, ciblée ou temporaire, demandée par les autorités judiciaires luxembourgeoises lorsque cela est nécessaire pour sauvegarder la sûreté, la défense, la sécurité publique et pour la prévention, la recherche, la détection et la poursuite d'infractions pénales." (188).

Le nouvel article 43-9 de la loi n°86-1067 du 30 septembre 1986 relative à la liberté de communication modifiée par la loi du 1^{er} août 2000 (189) prescrit des obligations à la charge des prestataires de services de l'internet. Cet article énonce : " Les prestataires mentionnés aux articles 43 -7 et 43-8 (les fournisseurs d'accès à des services de communication en ligne autres que de correspondance privée et les fournisseurs d'hébergement) sont tenus de détenir et de conserver les données de nature à permettre l'identification de toute personne ayant contribué à la création de contenu des services dont elles sont prestataires. Ils sont également tenus de fournir aux personnes qui éditent un service de communication en ligne autre que de correspondance privée des moyens techniques permettant à celles -ci de satisfaire aux conditions d'identification prévues à l'article 43-10 (v. supra). Les autorités judiciaires peuvent requérir communication auprès des prestataires mentionnés aux articles 43-7 et 43-8 des données mentionnées au premier alinéa. Les dispositions des articles 226 -17, 226-21 et 226-22 du code pénal sont applicables au traitement de ces données. Un décret en Conseil d'Etat, pris après avis de la Commission nationale de l'informatique et des libertés, définit les données mentionnées au premier alinéa et détermine la durée et les modalités de leur conservation." (190)

Cette obligation d'identification constitue une nouvelle donnée fondamentale pour la mise en œuvre de la responsabilité des auteurs d'infractions pénales. Les consultations menées sur la conservation des données par les pouvoirs publics auprès des praticiens concernés ont mis en évidence des divergences d'appréciation. L'Etat entend préserver les moyens d'identification les plus larges et le plus longtemps possible, alors que les prestataires de services, essentiellement en raison des coûts qui risquent d'affecter leur rentabilité, entendent les conserver pendant un délai minimum. La fourchette initiale allait de 1 à 12 mois. Il semblerait que le décret prévu à l'article 43-9 ne voit jamais le jour, car le Gouvernement a prévu d'apporter quelques modifications à ce texte lors de la présentation du projet de loi sur la société de l'information en 2002. Cependant, sur le plan des modalités, il faut impérativement que les données d'identification soit admises en preuve et qu'elles soient restituables au juge.

Une récente ordonnance de référé du TGI de Paris du 20 septembre 2000 a fait une première application de cette obligation en décidant que le fournisseur d'hébergement avait satisfait à ses obligations légales telles que découlant des dispositions de l'article 43-9 de la loi n°2000-719 du 1^{er} août 2000, envers la société demanderesse. En l'espèce, deux sites hébergés anonymement chez un fournisseur portaient préjudice à un fournisseur d'accès également opérateur de télécoms, en présentant des propos outranciers à son encontre et en portant atteinte à ses droits sur ses marques et à ses droits d'auteur. La partie demanderesse reprochait à l'hébergeur de ne pas avoir pris les mesures appropriées de nature à mettre un terme au trouble manifestement illicite et de ne pas lui avoir fourni l'identité et les coordonnées des auteurs responsables des sites. Les motifs de l'ordonnance étaient les suivants : " dès réception de la mise en demeure de One Tel, Multimania en a informé ses abonnés ; que dès la délivrance de l'assignation, elle a suspendu provisoirement les sites litigieux, dont l'un ONETELFUCK s'est d'ailleurs fait héberger par Géocities ; qu'à la réception de l'ordonnance sur requête du Président du tribunal de commerce, elle a fourni à la société One Tel les informations qu'elle détenait sur les sites en cause ; qu'elle a notamment communiqué à One Tel le journal des connexions de ses abonnés ; que ce journal faisait apparaître la société One Tel comme fournisseur d'accès des titulaires des sites hébergés par Multimania ; qu'en l'état de cette information, la société One Tel qui détenait elle-même des informations précises sur ses abonnés était à même de procéder sans tarder à leur identification et en conséquence de prendre à leur encontre les initiatives de nature à mettre un terme au trouble qu'elle dit subir ; qu'en permettant à One Tel de prendre connaissance de sa qualité de fournisseur d'accès des sites litigieux, la société Multimania a incontestablement satisfait à l'obligation légale de fourniture des données de nature à permettre l'identification d'une personne ayant contribué à la création d'un contenu de service dont elle est prestataire." (191).

A la vérité, ce texte entraîne moult incertitudes, contraires à la sécurité juridique. Par exemple, on ne sait pas quelles sont les données d'identification visées, quelles sont la durée et les modalités de leur conservation (192). On voit mal l'utilité de ces dispositions dans la mesure où l'on disposait de l'article 10 du NCP pour l'obtention des informations par le juge et de l'article 1382 c. civ. comme fondement de la responsabilité civile. De plus, la valeur d'ordre public de l'article 1382 c. civ. risque de venir heurter le principe de non responsabilité des fournisseurs d'hébergement (193).

2) Prestataires de services de certification (P.S.C.)

L'article 6 de la directive du 13 décembre 1999 pose les principales règles de responsabilité qui pèsent sur les prestataires de services de certification, y compris les moyens concrets dont ces prestataires disposent afin de limiter ou d'exonérer leur responsabilité en inscrivant dans les certificats électronique d'identification qu'ils émettent leurs limites d'utilisation et le montant maximum de la transaction sous -jacente (194). Cependant ce dernier point relatif à la limitation de leur responsabilité civile vis -à-vis des tiers au contrat qui les lient à leurs abonnés (les parties qui se fient), n'a, pour l'heure, pas encore fait l'objet de

dispositions pour leurs transpositions. Elles doivent, en principe, figurer dans la future Loi sur la société de l'information.

Le P.S.C. devra conserver les éléments d'identification de la personne titulaire du certificat qu'il a émis. Ces données d'identification sont collectées au moment de l'enregistrement de l'abonné par l'autorité d'enregistrement (elle peut être soit interne, soit externe au PSC). Généralement, les procédures d'enregistrement sont décrites dans la Déclaration des pratiques de certification "D.P.C." du P.S.C. Les pièces ayant servi à l'enregistrement de la personne varient en fonction de la classe de certificat en cause. A chaque classe de certificat est associé un niveau de sécurité, différents selon les besoins de l'abonné. L'enregistrement peut s'effectuer entièrement en ligne (niveau le plus bas car le PSC ne vérifie que l'adresse IP de l'abonné), elle peut s'effectuer en ligne avec envoi des copies certifiées conformes ou non des pièces justificatives par la Poste (pièces d'identité officielle, quittance attestant d'une adresse physique, ...), le niveau de sécurité est qualifié de moyen. Enfin, le contrôle de l'identité peut être réalisé en face à face avec les pièces exigées aux bureaux de l'autorité d'enregistrement, voire, on peut envisager que ce contrôle physique ne s'effectue que lors du retrait du certificat et de ses données d'activation initiales. Cependant, force est de constater que le P.S.C. doit "enregistrer toutes les informations pertinentes concernant un certificat électronique pendant le délai utile, en particulier, pour pouvoir fournir une preuve de la certification en justice. Ces enregistrements peuvent être effectués par des moyens électroniques." Cette disposition est parfaitement justifiée, ne fût-ce que pour être en mesure de justifier l'identité de la personne titulaire du certificat ou de permettre au P.S.C. d'apporter la preuve qu'il a été diligent. Dans une perspective pénale, le P.S.C. devra fournir les données d'identification collectées lors de l'enregistrement, spécialement si la personne a utilisé un pseudonyme.

Toutes ces données d'identification devront bien entendu faire l'objet des déclarations relatives aux fichiers et à leurs traitements auprès de la C.N.I.L.

Aux termes de la directive, le P.S.C. doit s'identifier et faire état du pays dans lequel il est établi ([\[95\]](#)). Au surplus, si l'article 7 c) du projet de décret transposant le c) de l'Annexe I de la directive sur la signature électronique impose aux P.S.C. de permettre aux personnes d'utiliser des pseudonymes en ces termes : " *tout certificat qualifié doit comporter : c) le nom du signataire ou un pseudonyme qui est identifié comme tel* ", on observera que seuls les certificats qualifiés sont assujettis à cette disposition. Une telle formulation oblige le P.S.C. à mentionner dans le certificat que le nom employé par le signataire est un pseudonyme. De cette façon, la personne qui se fie à une signature électronique sera informée du fait que le signataire du message électronique possède une identité réelle différente de celle qui figure dans le certificat électronique. L'article 8 de la directive prévoit que les P.S.C. doivent satisfaire aux exigences de la directive du 24 octobre 1995. Cet article sera transposé en même temps que la directive relative à la protection des données à caractère personnel. Enfin, le § 3 de l'article 8 dispose que " *sans préjudice des effets juridiques donnés aux pseudonymes par la législation nationale, les Etats membres ne peuvent empêcher le prestataire de service de certification d'indiquer dans le certificat un pseudonyme au lieu du nom du signataire.*" Ne peut-on pas y voir une consécration communautaire, à l'instar de l'article 43-10-II de la loi du 1^{er} août 2000, d'un droit à l'anonymat dans la société de l'information ?

Selon M. Lawrence Lessig, la régulation s'effectue via l'architecture des réseaux et elle porte plus particulièrement sur les certificats numériques d'identification. Le développement de ces passeports numériques conduirait, entre autres choses, à la fin de l'anonymat sur les réseaux ([\[96\]](#)). Les certificats permettront le filtrage de l'accès aux sites pour adultes (« *kids-ID* » v. « *adult-ID* »), voire de contrôler l'entrée sur le site en vérifiant que la personne détient le bon certificat ([\[97\]](#)) ou les droits nécessaires (ex : niveau de solvabilité). Les gouvernements « *could create incentives to enable digital IDs, not by regulating individuals directly but by regulating intermediaries. Intermediaries are fewer, their interests are usually commercial, and they are ordinarily pliant targets of regulation* » ([\[98\]](#)). En définitive, les quelques réflexions développées sur les rapports entre l'anonymat et le commerce électronique sont loin d'épuiser le débat dans un domaine qui n'en est encore qu'à ses balbutiements.

Notes :

[\[1\]](#) Dictionnaire Le Robert, V° « Anonymat » et « Anonyme ».

[\[2\]](#) Sous la direction de Gérard Cornu, Association Henri Capitant, *Vocabulaire Juridique*, Paris, Quadrige/P.U.F., 2000, V° « Anonyme ».

[\[3\]](#) Conseil d'État, *Internet et les réseaux numériques*, Paris, La documentation française, 1998, v. 47.

[\[4\]](#) « *On ne voit ni n'entend ceux avec qui on communique. Peu importe même, avec qui nous communiquons : nous ne voulons pas établir une relation, nous recherchons un effet. Or, dès qu'il n'a plus de pression sociale, l'une des principales raisons qui incite l'individu à tenir ses promesses et à honorer d'autres obligations disparaît. Il ne risque plus d'être puni par la déception qu'il a causé à ceux qu'il aime ou dont il dépend. De ce point de vue, on peut donc dire qu'il y a une érosion de la morale* », Christina Hultmark, *Développer des systèmes juridiques et une bonne moralité pour l'Internet*, in *Les dimensions internationales du droit du cyberspace*, Paris, éd. U nesco et Economica, 2000, p. 272.

[\[5\]](#) Pierre Kayser, *Le secret de la vie privée et la jurisprudence civile*, in *Mélanges Savatier*, 1965, p.406 ; Robert Badinter, *Le droit au respect de la vie privée*, J.C.P. 1968, I, 2136 ; Pierre Kayser, *La protection de la vie privée*, Paris, Economica, 1994 ; R. Lindon, J.-Cl. Civil, v. *Article 9*.

[\[6\]](#) Jacqueline Pousson Petit, *Le droit à l'anonymat*, in *Mélanges dédiés à Louis Boyer*, Presse de l' Université des sciences sociales de Toulouse, 1996, p.595 s.

[\[7\]](#) « *La libre communication des pensées et des opinions est un des droits les plus précieux de l'homme : tout citoyen peut donc parler, écrire, imprimer librement, sauf à répondre de l'abus de cette liberté dans les cas déterminés par la loi.* » Ce principe est également affirmé dans plusieurs textes internationaux : l'article 19 de la Déclaration universelle des droits de l'Homme du 10 décembre 1948, l'article 19-2 du Pacte international relatif aux droits civils et politiques du 19 décembre 1966 (le Pacte a été ratifié par la France à l'issue de la loi

n°83-461 du 25 juin 1980 et publié au J.O. par le décret n°81-77 du 29 janvier 1981 ; il est entré en vigueur le 4 février 1981) et l'article 10 de la Convention européenne de sauvegarde des droits de l'homme du 4 novembre 1950. Enfin, lors du sommet européen de Nice (7-9 décembre 2000), aux termes de l'article 7 de la Charte des droits fondamentaux de l'Union européenne, « *Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de ses communications* ». Pour le projet de Charte, v. Gaz. Pal. 29-31 octobre 2000, p. 30 s. ; Le Monde du 17 octobre 2000, p. 8. Sophia Koukoulis-Spilliotopoulos, *De Biarritz à Nice : le projet de Charte des droits fondamentaux est-il bien articulé avec le droit de l'Union ?*, Gaz. Pal. 29-31 octobre 2000, p. 18 s.

[8] Sur ce point, v. Alain Richard, *La liberté de communication*, in *La protection des droits fondamentaux*, Actes du Colloque organisé à Varsovie par les Facultés de droit de Varsovie et de Poitiers (9-15 mai 1992), Paris, P.U.F., 1993, p. 146 s. Cet auteur cite la définition donnée par Francis Le Balle, *Médias et sociétés*, Paris, 6^{ème} éd., Montchrestien, p. 234 : « *la liberté de communication, est le droit pour chacun, d'utiliser librement le média de son choix pour exprimer sa pensée en la communiquant à autrui, ou pour accéder à l'expression de la pensée d'autrui, quelle que soit, dans les deux cas, la forme ou la finalité de cette expression* ». op. cit., p. 146.

[9] Jacques Robert et Jean Duffar, *Droit de l'homme et libertés fondamentales*, Paris, Montchrestien, 7^{ème} éd., 1999, v. p. 429.

[10] Jacques Robert et Jean Duffar, *Droit de l'homme et libertés fondamentales*, op. cit., v. p. 429 s.

[11] Trib. Correctionnel de Paris, 2 novembre 2000. V. le point de vue de Lucien Rapp, *Secret des correspondances et courriers électroniques*, D. 2000, n°41, p. III s.

[12] Article 28 de la Loi n°90-1170 du 29 décembre 1990 sur la réglementation des télécommunications. Eric A. Caprioli, *Le nouveau régime de la cryptologie (suite aux décrets du 24 février 1998)*, Cah. Lamy du dr. de l'informatique, Mars 1998, n°101, fasc. K, p. 1 s. La Loi sur la société de l'information comportera un chapitre sur la liberté d'utilisation de la cryptologie ; sa présentation en conseil des ministres est prévue pour le printemps 2001. Ces modifications ont été annoncées par le Premier ministre dans son programme d'action pour l'entrée de la France dans la société de l'information en janvier 1999. Un dispositif réglementaire a libéralisé l'utilisation de moyens de cryptologie à des fins de confidentialité jusqu'à 128 bits (décrets du 17 mars 1999, J.O. du 19 mars 1999, p. 4050 s.).

[13] Serge Parisien et Pierre Trudel (avec la collaboration de Véronique Wattiez-Larose), *L'identification et la certification dans le commerce électronique*, Québec, éd. Yvon Blais, 1996 ; Eric A. Caprioli, *Sécurité et confiance dans le commerce électronique (signature numérique et autorité de certification)*, J.C.P. 1998, éd. G, I, 123 ; Eric A. Caprioli, *La loi française sur la preuve et la signature électroniques dans la perspective européenne – Directive 1999/93/CE du Parlement européen et du Conseil du 13 décembre 1999*, J.C.P. 2000, éd. G, I, 224.

[14] Jean Carbonnier, *Droit civil, I/ Les personnes*, Paris, P.U.F., 1996, n°35 (p.65) et Gérard Cornu, *Droit civil, Introduction, Les personnes, Les biens*, Paris, Montchrestien, 7^{ème} éd., 1994, v. n°611, p.231.

[15] Citant l'Avocat général Dontenville : " *le droit à l'anonymat est une expression très raffinée, en ce monde si dur, de la liberté individuelle*" (Conclusions sous Cass. crim. 25 avril 1985, Gaz. Pal. 28-29 juin 1985), J. Pousson-Petit, art. préc. note n° 6, v. p.597-598.

[16] Philippe Malaurie et Laurent Aynes, *Les personnes, Les incapacités*, Paris, Cujas, 5^{ème} éd., 2000, n°297, p.129-130.

[17] V. les développements de Mme Pousson Petit, *Le droit à l'anonymat, art. préc. supra note n°6*, p.599 s.

[18] « *L'objectif essentiel du droit au respect de l'anonymat est de préserver la tranquillité des personnes. (...) cette finalité est atteinte par la protection de deux valeurs fondamentales que sont l'identité et l'intimité*. » Jean-Christophe Saint-Pau, *L'anonymat et le droit*, Thèse, Université Montesquieu-Bordeaux IV, 1998, Tome 2, v. n°463. M. Richard Desgorces, il serait opportun de reconnaître un droit à l'anonymat. « (...) *séparé de la vie privée, l'anonymat comme l'image deviendrait une prérogative individuelle. Chacun aurait un droit subjectif au respect de son anonymat qu'il pourrait opposer aux tiers, mais seulement dans les limites fixées par le droit objectif*. » Note sous T.G.I. Paris, 24 mars 1999, C.omm. Com. élect. n°1, Octobre 1999, v. p. 22-23.

[19] Xavier Linant de Bellefonds, préface à l'ouvrage de André Bertrand, *Droit à la vie privée et droit à l'image*, Paris, Litec, 1999, v. p. XI.

[20] cf. Loi du 1^{er} août 2000.

[21] Claude Lévi-Strauss, dans *la pensée sauvage*, décrit plusieurs systèmes d'attribution du nom dans des sociétés « primitives », par exemple, « *un enfant est connu par son nom propre jusqu'à ce que meure un de ses ascendants. (...) chez les germains, un enfant est appelé par son nom si tous ses frères et sœurs sont vivants* », Paris, Plon, 1962, v. p. 230.

[22] Jean-Christophe Saint-Pau, *L'anonymat et le droit*, Thèse préc., Tome 2, v. n°864.

[23] V. avec intérêt l'étude de Etienne Davio, *Anonymat et autonomie identitaire sur Internet*, in Cahiers du C.R.I.D., sous la direction de Etienne Montero, *Droit des technologies de l'information, Regards prospectifs*, Bruxelles, Bruylant, 1999, p. 303 s.

[24] Bernard Edelman, *La personne en danger*, Paris, P.U.F., 1999.

[25] Directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000, *relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur* (« *directive sur le commerce électronique* »), J.O.C.E. L.178/1 du 17 juillet 2000. V. Jérôme Huet, *La problématique du commerce électronique au regard du projet de directive communautaire du 23 décembre 1998*, *Communic., C.omm. Elect.*, décembre 1999, p.9 s.

[26] Etienne Davio, art. préc. supra note n°23, v. p.307.

[27] Etienne Davio, art. préc. supra note n°23, v. p.307 s.

[28] V. <http://www.eqosurf.com>, et <http://www.google.com>

[29] Sur la question, v. particulièrement les travaux de Jean-Marc Dinant, *Les traitements invisibles sur internet*, Cahiers du CRID, Bruxelles, Bruylant, n°16, 1999, p.277-302, disponible en ligne : <http://www.droit.fundp.ac.be/crid/eclip/Luxembourg.html>. (1998) ; égal. Du même auteur : *Le visiteur visité*, disponible sur le site : <http://www.lex-electronica.org/articles/v6-2/dinant.htm>.

- [30] La Gazette des communes, 15 novembre 1999, fasc. 2, n° 43 -1525, p.113. Par la suite, la commune n'a pas interdit l'accès libre à la bibliothèque, mais elle exige désormais la présentation d'une carte de lecteur et que les utilisateurs demandent la souris avant de se connecter à l'Internet.
- [31] Cela correspond à la famille des protocoles Internet utilisés.
- [32] Cette adresse est composée de quatre octets (32 bits) généralement exprimée sous forme décimale. V. Arnaud Dufour, *Internet, Que sais-je ?*, Paris P.U.F., 2^{ème} éd., 1996, p.117.
- [33] Selon M. Richard Desgorces, « *Derrière son ordinateur, la vie privée d'un individu est a priori bien protégée (l'ordinateur n'est pas une caméra qui permet à l'interlocuteur de voir à l'intérieur d'un appartement), en revanche son anonymat l'est beaucoup moins, puisque son nom est un élément de son adresse internet.* » Note sous T.G.I. Paris, 24 mars 1999, Comm. Com. élect. N°1, Octobre 1999, v. p. 22-23.
- [34] Pierre-Yves Gautier, *L'e-mail*, in Université Panthéon-Assas, *Clés pour le siècle*, Paris, Dalloz, 2000, p. 375.
- [35] Cédric Manara, *Commerce d'identités électroniques*, D. 2000, n°37, p.111.
- [36] Lucien Rapp, *Le courrier électronique*, Paris, PUF, Que sais-je ?, 1998 ; Cédric Manara, *Aspects juridiques de l'e-mail*, D. Affaires 1999, p.278 ; Pierre-Yves Gautier, *L'e-mail, art. préc.*, v. p. 369.
- [37] En ce sens, Grégoire Loiseau, *Le nom de domaine et Internet : turbulences autour d'un nouveau signe distinctif*, D. 1999, Chr., p. 247 ; Jean-Christophe Galloux, *Droit de la propriété industrielle*, Paris, Dalloz, 2000, n°1301.
- [38] Pierre-Yves Gautier, *L'e-mail*, art. préc., v. p. 372-374.
- [39] Jean-Marc Dinant, *Le visiteur visité*, disponible sur le site : <http://www.lex-electronica.org/articles/v6-2/dinant.htm>, v. p.8.
- [40] Paul Didier, *Monnaie de compte et compte bancaire*, in *Etudes offertes à Jacques Flour*, Paris, Defrénois, 1979, v. p.139
- [41] Jean Carbonnier, *Droit civil, 1/Les personnes, op. cit.*, v. n°35, p.65 : « *Le droit contemporain, toutefois – policier sans se l'avouer – restreint le principe de l'anonymat dans la mesure où il rend obligatoire le paiement par chèque.* »
- [42] Loi de finances pour 2001 du 30 décembre 2000, n°2000-1352. Les particuliers non commerçants devaient déjà payer par chèque barré (ou virement, TIP, carte de paiement) les biens ou services d'un montant supérieur à 50.000 francs (LF pour 1999 n°98-1266 du 30 décembre 1998, J.O. du 31 décembre 1998) sous peine d'une amende fiscale de 100.000 francs (article 1749 C.G.I.). Le phénomène est d'autant plus marquant que le montant était fixé à 150.000 francs en 1998 !
- [43] Pour les loyers, transports, services, fournitures, travaux ou les règlements afférents à des acquisitions d'objets mobiliers ou d'immeubles ainsi que le paiement des produits de titres nominatifs supérieurs à 5.000 francs doit s'effectuer par chèque, effet de commerce, compensation ou passation en compte courant, mais le paiement en espèces est interdit (Cass. Com. 24 janvier 1977, Bull. Civ. IV, n°18, p.15).
- [44] J.O.C.E. L 275 du 27 octobre 2000, p.39 s.
- [45] V. l'article 1 § 3 - b de la directive du 18 septembre 2000 préc.
- [46] Sous la direction de Christian Galvalda et Pierre Sirinelli, *Lamy Droit des médias et de la communication*, V° « *Commerce électronique* », Etude n°468 (novembre 2000), spéc. n°468-157 s. (par Eric A. Caprioli, Anne Cantero et Xavier Le Cerf).
- [47] Conseil d'état, *Internet et les réseaux numériques*, op.cit., v. 47-48.
- [48] V. la page d'accueil du programme LPWA de la société Lucent Technology sur le site : <http://www.lpwa.com>.
- [49] V. spéc. l'un des sites le plus connu en matière d'anonymat : <http://www.anonymizer.com>.
- [50] Si l'on fait plusieurs requêtes en ligne auprès des principales bases de brevets, on constate un nombre très important de dépôts de brevets relatifs à la protection de l'anonymat, sous des formes très diverses, sur les réseaux numériques.
- [51] Jean Carbonnier, *Droit civil, Les personnes, op. cit.*, v. n°82 s.
- [52] P. Népveu, *Du pseudonyme*, JCP 1961, éd. G, I, 1662 ; J.-M. Leloup, *Le pseudonyme*, R.T.D.civ. 1963, p.449 ; J. Penneau, *L'utilisation d'un pseudonyme par les membres des professions médicales, propos sur une réponse ministérielle*, JCP 1985, éd. G, I, 3185 ; Grégoire Loiseau, *Le nom objet d'un contrat*, Paris, L.G.D.J., Bibl. dr. privé, t. 274, Préface de Jacques Ghestin, 1997, v. spéc. les n°31 et 161.
- [53] Anne Lefebvre-Teillard, *Introduction historique au droit des personnes et de la famille*, Paris, P.U.F., 1996, v. n°54, p.71.
- [54] H., L. J. Mazeaud et François Chabas, *Leçons de droit civil, Les personnes*, 8^{ème} éd. par Florence Laroche-Gisserot, Paris, Montchrestien, 1997, v. n°548.
- [55] T.G.I. Paris, 5 juillet 1995, D. 1996, p.174, note J. Ravanas ; Paris, 15 septembre 1999, D. 2000, Jp, p.801, note Philippe Bonfils.
- [56] Cass. civ. 1^{ère}, 19 février 1975, D. 1975, p.411, note R. L..
- [57] Paris, 5 juillet 1979, Gaz. Pal. 1980, 1, p.21.
- [58] Sur l'usage d'un faux nom, Gérard Cornu, *Droit civil, Introduction, Les personnes, Les biens*, Paris, Montchrestien, 7^{ème} éd., 1994.
- [59] Gérard Cornu, *Droit civil, Introduction, Les personnes, Les biens*, op.cit., v. n°611.
- [60] Sur les oeuvres anonymes et les oeuvres pseudonymes, v. Georges Bonnet, *L'anonymat et le pseudonyme en matière de propriété littéraire et artistiques*, Thèse, Paris, 1966 ; André Lucas et Henri-Jacques Lucas, *Traité de la propriété littéraire et artistique*, Paris, Litec, 2^{ème} éd., 2001, v. n°405-406 ; Pierre-Yves Gautier, *Propriété littéraire et artistique*, Paris ; P.U.F., 3^{ème} éd. 1999, n°100.
- [61] Bernard Teyssié, *Droit civil, Les personnes*, Paris, Litec, 3^{ème} éd., 1998, v. n°166, p.122.
- [62] V. Conseil constitutionnel, Décision n°94-352 du 18 janvier 1995 sur la loi d'orientation et de programmation relative à la sécurité, où la méconnaissance du droit au respect de la vie privée « peut être de nature à porter atteinte à la liberté individuelle ». Egal. la décision n°99-416 du 23 juillet 1999 sur la loi portant création d'une couverture maladie universelle, la liberté que l'on trouve à l'article 2 de la Déclaration des droits de l'homme « implique le respect de la vie privée. » (J.O. du 28 juillet 1999, p.11253).

- [63] Jean Pradel, *Les dispositions de la loi n°70-643 du 17 juillet 1970 sur la protection de la vie privée*, D. 1971, chr. XVIII, p.3 ; Pierre Kayser, *La protection de la vie privée, protection du secret de la vie privée*, Paris, Economica, 3^{ème} éd., 1995 ; François Rigaux, *La protection de la vie privée et des autres biens de la personnalité*, Bruxelles, Bruylant et Paris L.G.D.J., 1990 ; André Bertrand, *Droit à la vie privée et droit à l'image*, Paris, Litec, 1999, v. n° 147 s. ; Guy De Vel, *Le Conseil de l'Europe, la vie privée et la protection des données, in Vie privée : nouveaux risques et enjeux*, C.H.R.I.D. 1997, n° 13, p. 17 s. Louise Cadoux et Pierre Tabatoni, *Les défis d'Internet à la protection de la vie privée : institutions, marchés et techniques en Europe et aux Etats-Unis, in La protection de la vie privée dans la société de l'information*, Groupe d'études Société de l'information et vie privée, coordinateur Pierre Tabatoni, Paris, P.U.F., Tome 1, 2000, p.15 s.
- [64] Jean-Claude Soyer, *L'avenir de la vie privée (face aux effets pervers du progrès et de la vertu ...)*, in *Mélanges en hommage à François Terré*, Paris, Dalloz.U.F.- éd. du Juris-Classeur, 1999, v. p.345, article également publié in *La protection de la vie privée dans la société de l'information*, Groupe d'études Société de l'information et vie privée, coordinateur Pierre Tabatoni, Paris, P.U.F., Tome 1, 2000, p. 9 s.
- [65] V. à titre d'illustration les sites qui proposent, contre paiement, la possibilité de « partager » 24 heures sur 24, la vie de plusieurs prétendues étudiantes américaines.
- [66] C.N.I.L, *Dix ans d'informatique et libertés*, préface de Jacques Fauvet, Paris, Economica, 1988 et Jean Frayssinet, *Informatique, fichiers et libertés*, Paris, Litec, 1992.
- [67] V. par exemple : Conseil constitutionnel, décision n°98-405 DC du 29 décembre 1998 validant l'article 107 de la Loi de finances pour 1999. Jacques Robert et Jean Duffar, *Droit de l'homme et libertés fondamentales*, op. cit., v. p. 436 s. Ces auteurs précisent que l'avis favorable donné par la C.N.I.L. était limité à « l'usage du numéro à la vérification de l'identité et de l'adresse des contribuables ».
- [68] Guy Braibant, *Données personnelles et société de l'information*, Paris, La Documentation française, 1998.
- [69] Décision de la Commission du 26 juillet 2000, conformément à la directive 95/46/CE du Parlement européen et du Conseil relative à la pertinence de la protection assurée par les principes de la « sphère de sécurité » et par les questions souvent posées y afférentes, publiées par le ministère du commerce des Etats - Unis d'Amérique, J.O.C.E. L 215 du 25 août 2000, p.7.
- [70] Jean Frayssinet, *Le rapport de la « mission Braibant » sur la transposition de la directive relative à « la protection des données personnelles » du 24 octobre 1995*, Cahiers Lamy Droit de l'informatique et des réseaux, n°103, Mai 1998, fasc. B, v. p.11.
- [71] Lamy Droit de l'informatique, Formulaires, v. III -155. Selon la Charte, l'utilisateur est " toute personne accédant à l'Internet, aux seules fins de consultation ou de correspondance privée. L'utilisateur ainsi entendu n'est pas soumis aux obligations de la présente charte".
- [72] V. la charte Yahoo ! France sur le respect de la vie privée, http://fr.docs.yahoo.com/info/privacy_hyml (site consulté le 24/01/2001).
- [73] V. l'exemple de la société Vivendi Universal : <http://www.vivendi.com/text/vu/en/privacy.html>, où après s'être engagée à ne pas collecter de données personnelles telles que le nom ou l'adresse électronique (article 1), l'article 5 « Use of IP addresses » mentionne : « Vivendi Universal collects IP addresses for the purpose of its system administration and to analyse the use of its Site. We do not link IP addresses to any information that is personally identifiable, which means that your session will be logged, but you remain anonymous to us. We may use your IP addresses in cooperation with your Internet service provider to identify you if we feel it is necessary to enforce compliance with our terms of use or to protect our services, customers or as required by law. »
- L'article 4 intitulé " Use of cookies " dispose : « Cookies are pieces of information that a website transfers to an individual's computer hard drive for record keeping purposes. Cookies are not used by this Site but may be used on other sites accessible from our Site. » Le site français de cette société, à la date du 9 janvier 2001, ne comportait pas de telles dispositions, réservées à l'international. Sans doute cela s'explique-t-il par le caractère impératif des obligations légales des dispositions de la loi du 6 janvier 1978.
- [74] Cass. crim. 24 mars 1949, Bull. crim. n°144.
- [75] P. Bouzat, *La loyauté dans la recherche de la preuve*, in *Mélanges Hugueney*, 1964, p.155 s ; Christophe Galloux, *L'empreinte génétique : la preuve parfaite ?*, JCP 1991, éd. G, I, 3497 ; G. Danjaume, *Le principe de la liberté de la preuve en procédure pénale*, D. 1996, Doct., p.153.
- [76] Le texte du projet est consultable sur le site : <http://conventions.coe.int/treaty/fr/projets/cybercrime.htm>. Egal. notre chronique : Rev. dr. banc. fin. n°3, mai-juin 2000, p.167.
- [77] Le libellé de cet article est tiré du Projet de convention sur la cyber-criminalité, Version PC-CY (2000) Projet n°24 Rév. 2 en date du 21 novembre 2000.
- [78] Le titre de l'article 16 dans sa version antérieure était le suivant : « Conservation rapide de données stockées dans un système informatique ».
- [79] Selon l'article 1 -d du projet de convention, de telles données de connexion aux réseaux désignent : « toutes données ayant trait à une communication passant par un système informatique, produites par ce dernier en tant qu'élément de la chaîne de communication, avec indication des informations suivantes : origine, destination, itinéraire, heure, date, taille et durée de la communication ou type de service (réseau) sous - jacent. » (Projet n°24 Rév. 2).
- [80] V. l'article précurseur sur la question de la mutation de l'identité et de la façon d'être nommer, Philippe Lemoine, *L'identité informatisée*, in *Les enjeux culturels de la société de l'information*, Paris, La documentation française, 1980, p.27 s.
- [81] Alain Bernard, *L'identité des personnes physiques en droit privé, remarques en guise d'introduction*, in *L'identité politique*, Centre Universitaire de Recherches Administratives et Politiques de Picardie, P.U.F., 1994, v. p. 128.
- [82] Jean-Marie Benoist, *Facettes de l'identité*, in *L'identité*, Séminaire dirigé par Claude Lévi - Strauss, Paris, P.U.F. 3^{ème} éd. Quadrige, 1995, p.17.
- [83] V. la charte Yahoo ! France sur le respect de la vie privée http://fr.docs.yahoo.com/info/privacy_hyml (site consulté le 24/01/2001), où après avoir pris l'engagement de ne jamais divulguer les données personnelles des

utilisateurs, sauf avec leur autorisation ou dans des circonstances très particulières, « Yahoo ! peut aussi être amené à divulguer des informations confidentielles dans des circonstances particulières, lorsque leur divulgation est nécessaire à l'identification, à l'interpellation ou à la poursuite en justice de tout individu susceptible de porter préjudice ou atteinte (intentionnellement ou non) aux droits ou à la propriété de Yahoo !, à d'autres utilisateurs Yahoo !, ou à toute autre personne risquant d'être pénalisée par de telles activités. Yahoo ! peut enfin divulguer des données personnelles lorsque Yahoo! ... » v. p.4.

[84] Eric A. Caprioli, *Ecrit et preuve électroniques dans la loi n°2000-230 du 13 mars 2000*, J.C.P. 2000, éd. E, Cah. Dr. de l'entr. N°2, suppl. n°30 du 23 juillet 2000 et *Traçabilité et droit de la preuve*, Droit & Patrimoine 2001 (à paraître dans les actes du colloque de Toulon organisé par le CERANT, 4-5 mai 2000 sur la "Traçabilité"). Jérôme Huet, *Vers une consécration de la preuve et de la signature électroniques*, D. 2000, chr., p.6 ; Pierre-Yves Gautier, *Le bouleversement du droit de la preuve : vers un mode alternatif de conclusion des conventions*, Petites affiches, 7 février 2000, n°26, p.10, n°16 et *Révolution internet : le dédoublement de l'écrit juridique*, D. 2000, n°12, Actualité, p.V -VI.

[85] Jean-François Renucci, *L'identité du cocontractant*, R.T.D.com. 1993, p. 442 s. ; Eric A. Caprioli, *Sécurité et confiance dans le commerce électronique, Signature numérique et autorité de certification*, J.C.P. 1998, éd. G, I, 123.

[86] Emmanuel Jez et Frédéric - Jérôme Pansier, *Responsabilité des hébergeurs à l'aune de la loi du 1^{er} août 2000*, Gaz. Pal. 8-9 septembre 2000, p. 19 s. En jurisprudence, v. notamment : Paris, 10 février 1999 (affaire : Valentin Lacambre c./ Estelle Halliday), Droit & Patrimoine, n°74, septembre 1999, obs. Eric A. Caprioli ; J.C.P. 1999, éd. E, I, n°22, obs. Michel Vivant et Christian Le Stanc ; T.G.I. Nanterre, 8 décembre 1999 (affaire Lynda Lacoste c./ Multimania et alii), Droit & Patrimoine, n°85, septembre 2000, p.106, obs. Eric A. Caprioli et Versailles 8 juin 2000, Légipresse n°174 - III, p.139, ote C. Rojinsky.

[87] Directive 2000/31/CE du 8 juin 2000, JOCE L. 178 du 17 juillet 2000. Cyril Rojinski, *Commerce électronique et responsabilité des acteurs de l'internet en Europe*, Gaz. Pal. 23-24 juin 2000, p.18 s. et *L'approche communautaire de la responsabilité des acteurs de l'internet*, Expertises, Octobre 2000, p.297 s.

[88] Loi du 14 août 2000, publiée au Mémorial (J.O. du Grand Duché de Luxembourg), Recueil de législation, A - n°96 du 8 septembre 2000, p.2176 s., pour les articles relatifs à la responsabilité des prestataires intermédiaires, v. p.2186-2187.

[89] Loi n°2000-719 du 1^{er} août 2000 modifiant la loi n°86-1067 du 30 septembre 1986 relative à la liberté de communication, J.O. du 2 août 2000, p.11903.

[90] Basile Ader, *La responsabilité des acteurs de l'internet après la loi du 1^{er} août 2000*, Légipresse, n°176, Novembre 2000, p. 113 ; Maryline Boizard, *La responsabilité en matière d'internet*, Droit & Patrimoine, n°89, Janvier 2001, v. p. 70 s.

[91] L'ordonnance du 20 septembre 2000, affaire Sarl One Tel c./ SA Multimania, est publiée sur les sites : <http://www.juriscom.net> et www.legalis.net/jnet ; Comm. Com. Electr. Décembre 2000, p.24, note Jean-Christophe Galloux.

[92] Une ordonnance de référé (inédite) du T.G.I. de Marseille, 4 octobre 2000, a condamné un hébergeur sous astreinte, à communiquer les données d'identification suivantes : « informations déclaratives communiquées par l'abonné au moment de son inscription au service ; journal de connexions FTP faisant notamment apparaître l'adresse IP affectée à la machine de l'utilisateur et la date et l'heure de connexion ».

[93] D'autres questions ne sont pas résolues : par exemple, l'article 43-7 de la loi du 1^{er} août 2000 s'applique-t-il aux employeurs qui disposent de serveurs et qui mettent des adresses électroniques à la disposition de leurs salariés ?

[94] Directive du 13 décembre 1999, JOCE L. 13 du 19 janvier 2000, p.12 s. Eric A. Caprioli, *La loi sur la preuve et la signature électroniques dans la perspective européenne*, JCP 2000, éd. G, I, 224 et *La directive européenne n°1999/93/CE du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques*, Gaz. Pal. 29-31 octobre 2000, p.5-17. Sur la signature électronique, v. égal. : Mireille Antoine et Didier Gobert, *Pistes de réflexion pour une législation relative à la signature digitale et au régime des autorités de certification*, Rev. Gén. Dr. Civ. Belge 1998, n°4/5, p.285 s. ; Etienne Davio, *Preuve et certification sur Internet*, Rev. Droit Com. (Belge), 1999, p.663 s. ; Michel Jaccard, *Le rôle, le statut et la responsabilité de l'autorité de certification dans la transmission de données signées numériquement*, in *Mélanges en l'honneur du Professeur François Dessemontet*, Cedidac n°38, Lausanne, 1998, p.403 s.

[95] Le certificat qualifié doit comporter : "b) l'identification du prestataire de service de certification ainsi que le pays dans lequel il est établi."

[96] Lawrence Lessig, *Codes and other laws of cyberspace*, Basic Books, New York, 1999. Cédric Manara, *La technique et le droit des réseaux : codes contre codes ?*, note bibliographique, Petites Affiches du 22 novembre 2000, p.14-15.

[97] Lawrence Lessig, *Codes and other laws of cyberspace*, op. cit., v. p.176.

[98] Lawrence Lessig, *Codes and other laws of cyberspace*, op. cit., v. p.50.