Chapitre II

L'anonymat

Le 21 septembre 1998, le quotidien Libération *publiait un article intitulé « Les nouveaux athlètes du travail ». Interrogé par une journaliste, un dirigeant de la société française Ubisoft, l'un des principaux éditeurs mondiaux de jeux vidéo, y exposait sa vision de l'entreprise moderne : une communauté d'hommes et de femmes concentrés sur la seule réussite commerciale de la société, sans soucis pour leur temps de travail et leurs acquis sociaux.*

En réaction à cet article, un « groupe de salariés » d'Ubisoft lançait, le 15 décembre 1998, le site Internet Ubifree[1]*. Le site fermera cent six jours plus tard, le 31 mars 1999. Entre-temps, il aura suscité beaucoup de commentaires et d'interrogations. L'idée maîtresse d'Ubifree était résumée dans le titre du message d'accueil : « Voici venu le temps du syndicat virtuel ».*

Dans une lettre ouverte à leur président, le « groupe de salariés » réagissait à l'article de Libération *: « Ces propos sont scandaleux. Ils laissent croire à un état d'esprit unanime, celui d'une collectivité de jeunes imbéciles prêts à tout pour assurer la réussite commerciale de l'entreprise, obsédés par son expansion, n'éprouvant que du mépris envers leurs droits sociaux les plus élémentaires. Et c'est là une représentation fantaisiste, mensongère, une représentation insultante à l'égard des employés de votre société. Vous*

1. Le site est accessible à titre d'archive à l'adresse *http://membres.lycos.fr/ubifree/*.

ignorez, sans doute, qu'un grand nombre d'entre eux sont très insatisfaits de leurs conditions de travail. D'ailleurs comment pourriez-vous en être informé, puisque la précarité de la plupart des emplois rend impossible toute forme d'expression individuelle et qu'il en va de même à l'échelle collective de par l'absence de représentation du personnel ? Monsieur [X (le dirigeant d'Ubisoft)], ni aucun responsable, n'est censé parler au nom de tous. Or le personnel d'Ubisoft n'a aucun moyen de se faire entendre. Cette situation est inacceptable. »

L'article introductif se concluait ainsi : « Ce site accueillera la parole de tous, employés et responsables. Nous nous chargerons de sa mise à jour hebdomadaire et assurerons, bien entendu, l'anonymat des intervenants. » Depuis lors, l'auteur des premières pages du site Ubifree a mis fin à son anonymat : après deux ans passés au sein de la société Ubisoft, il a démissionné et s'exprime régulièrement en public sur cette initiative[1].

Communiquer de la sorte, c'est-à-dire de manière anonyme, est-il légal ? L'anonymat sur Internet a ses partisans et ses détracteurs, et les débats entre les uns et les autres sont souvent passionnés. Doit-on et peut-on lutter contre l'anonymat sur Internet ? Doit-on rendre l'anonymat illégal ou, au contraire, doit-on l'ériger en droit ? Quel est le statut juridique de l'anonymat aujourd'hui, si toutefois il en possède un ?

Problématiques de l'anonymat

L'anonymat soulève des questions difficiles, sur les plans à la fois moral, philosophique et juridique[2]*. Ces questions prennent un relief particulier dans la société de l'information, dans laquelle les internautes, usagers du téléphone mobile, détenteurs d'une carte bancaire ou d'une carte téléphonique et demain d'une carte à puce sans contact RFID sont continuellement tracés. L'anonymat apparaît dès lors comme un recours possible contre les abus du traçage. À l'inverse, l'anonymat peut être un masque*

1. Pierre Mounier, « Jérémie Lefebvre : un rebelle chez Ubisoft », *www.homo-numericus.net.*
2. Éric Caprioli, *Anonymat et commerce électronique*, Actes des premières journées internationales du droit et du commerce électronique, octobre 2000.

derrière lequel développer toute une série d'actes portant atteinte aux droits de tiers (diffamation, injure) ou à l'ordre public.

Selon une première définition, agir de manière anonyme, c'est agir « sans laisser de trace[1] ». De ce point de vue, l'anonymat n'existe pas dans le monde numérique. La grande masse des utilisateurs des réseaux y laisse quantité de traces susceptibles d'être identifiantes. Par exemple, accéder à Internet, c'est obligatoirement disposer d'une adresse IP mise à disposition par un fournisseur d'accès. Cette adresse IP est enregistrée par les machines du réseau qui identifient de la sorte un titulaire, généralement un fournisseur d'accès, lequel sait lui-même à qui l'adresse IP a été attribuée. De même, téléphoner consiste le plus souvent à utiliser une ligne téléphonique qui identifie un abonné enregistré par un opérateur.

Selon une autre définition communément admise[2], l'anonymat consiste à « ne pas se déclarer l'auteur d'un fait, d'un écrit ». Dans le monde numérique, le recours à des pseudos ou à des adresses e-mail ne laissant apparaître aucune identité visible peuvent être les vecteurs d'une certaine anonymisation.

Notre propos n'est pas de nous livrer à une apologie de l'anonymat. Cependant, dans le contexte actuel de surveillance généralisée d'Internet, il faut reconnaître à l'anonymat la vertu de constituer une protection efficace pour l'individu et ses libertés. Rappelons toutefois que l'anonymat doit être utilisé dans les limites de la loi. L'anonymat est d'ailleurs tout relatif, puisqu'il peut être levé par les juges et les tribunaux, qui disposent de prérogatives fortes pour obtenir l'identification d'actes anonymes illégaux.

Les sept règles de l'anonymat sur Internet

Être anonyme n'est pas être dénué d'identité, mais refuser de divulguer son identité en la masquant. Pour y parvenir dans les réseaux numériques, il faut déployer quantité de ruses et d'efforts. Certains se cantonnent à n'utiliser que les accès publics à Internet (cybercafés, accès Wi-Fi publics, etc.). D'autres recourent à des machines distinctes, l'une réservée à un

1. Définition donnée par Thierry Nabeth et Mireille Hildebrandt, « Inventory of Topics and Clusters », in *Furure of Identity in the Information Society, www.fidis.net.*
2. Définition du dictionnaire Larousse universel.

usage anonyme et nettoyée systématiquement après usage de tous cookies et historiques, l'autre d'usage courant.

Pour les utilisateurs de compétence moyenne, voici quelques règles simples permettant d'obtenir un anonymat relatif sur les réseaux numériques.

1. Ne jamais révéler son identité

Pour agir anonymement, il convient autant que possible de ne pas révéler ni agir sous son identité réelle. De nombreux services ne requièrent aucune identification préalable, ni même de signature visible.

Visiter un site Web, une page personnelle ou un blog ne requiert pas d'identification préalable auprès de l'éditeur du site. Il est même possible d'interagir avec un service sans fournir d'identification. D'une manière générale, c'est le cas du Web dit 2.0, qui consiste en la mise en commun d'informations issues de contributeurs le plus souvent anonymes. Chacun peut y apporter une contribution non signée, qui apparaît comme anonyme, et seule l'adresse IP du contributeur est enregistrée. Une kyrielle d'autres services, tels que forums de discussion ou blogs, invitent leurs visiteurs à déposer des contenus (vidéo, audio, commentaire) sans exiger d'identification préalable.

Certains services sur le Web exigent une identification préalable. Pour rester anonyme, l'utilisateur du service n'a d'autre choix que de déclarer une identité et des attributs qui ne sont pas réels. Pour savoir si une telle manipulation est licite, l'utilisateur doit vérifier les conditions d'utilisation du service qu'il s'engage à respecter. Celles de DailyMotion, par exemple, n'exigent pas la déclaration d'une identité réelle[1]. En revanche, celles du service concurrent You Tube stipulent que « lorsque vous créez votre compte, vous devez fournir des informations complètes et exactes[2] ». On peut constater que cette disposition manque de précision puisqu'une identité peut être « complète et exacte » sans être nécessairement réelle. Selon nous, dès lors qu'un utilisateur fournit des informations qui le caractérisent, comme un pseudo, il se conforme aux conditions d'utilisation de You Tube.

1. *http://www.dailymotion.com/legal/privacy* (novembre 2007).
2. *http://fr.youtube.com/t/terms* (novembre 2007).

Si les conditions d'utilisation d'un service mentionnent l'obligation de déclarer « des informations exactes *et réelles* » permettant à l'éditeur du site d'entrer en contact avec l'utilisateur, le fait de déclarer une autre identité que l'identité réelle autoriserait l'éditeur du site à suspendre le service à l'utilisateur. En outre, si une fausse déclaration devait engendrer un préjudice envers l'éditeur du service ou un tiers, l'utilisateur pourrait être poursuivi et redevable de dommages et intérêts. Dans les cas extrêmes, la déclaration d'une fausse identité peut être considérée comme une escroquerie et relever du droit pénal *(voir le chapitre IV)*.

2. Utiliser un pseudo

Pour cacher son identité réelle, il est possible de recourir à un pseudonyme, ou pseudo, sans rapport avec l'identité réelle de son titulaire. On parle dans ce cas de « pseudonymat ». Le pseudo permet d'interagir avec le réseau sans révéler son identité réelle. Il est très facile de créer un blog sous un pseudo et de s'y exprimer librement sans dévoiler son identité réelle. Le célèbre blog « Journal d'un avocat » est ainsi signé de M^e^ Eolas[1], pseudonyme d'un avocat du barreau de Paris.

Précisons qu'un pseudonyme n'est pas toujours et automatiquement synonyme d'anonymat. Il n'est que de songer à l'emploi qu'en font les artistes. Il n'en reste pas moins que la pratique nouvelle du pseudo dans un but d'anonymat est désormais bien installée sur Internet.

3. Choisir un nom de domaine sans rapport avec son identité réelle

La plupart des noms de domaine Internet sont choisis librement. Les unités ou bureaux d'enregistrement de noms de domaine Internet diffusent des annuaires de ces noms de domaine.

Appelés « Whois », ces annuaires, le plus souvent librement accessibles en ligne, renseignent sur les noms des titulaires de noms de domaine Internet. En règle générale, les unités d'enregistrement imposent à ces titulaires de déclarer une identité réelle. Certaines de ces unités ne publient

1. *http://www.maitre-eolas.fr/*.

toutefois que partiellement l'identité déclarée par le titulaire d'un nom de domaine.

4. Recourir aux webmails

Les internautes peuvent utiliser des adresses e-mail sous forme de webmails. Les webmails sont des services d'adresses électroniques gratuites proposés par des sociétés telles que Yahoo !, Google Gmail ou Windows Live Mail (ex-Hotmail), pour ne citer que les plus emblématiques. Ils permettent à leurs usagers de gérer leur courrier à partir d'une interface Web. Les messages envoyés et reçus sont stockés sur les serveurs du fournisseur de service.

Le compte webmail nécessite un identifiant et un mot de passe choisis par le titulaire du compte. Pour bénéficier d'un tel compte, il suffit généralement de déclarer une identité quelconque, qui peut être un pseudo. Les conditions générales de service imposent souvent la déclaration d'une identité réelle, mais cette obligation contractuelle est peu respectée.

La sanction pour le défaut de déclaration réelle se limite à l'exclusion du service, sauf en cas de fraude. Yahoo ! France oblige l'internaute à accepter ses conditions générales de services avant de lui fournir une adresse webmail et un espace de stockage : « Vous vous engagez à i) fournir des informations vraies, exactes et complètes, et ii) les maintenir et les remettre à jour régulièrement. La fourniture de ces informations et leur maintien à jour de façon à permettre votre identification sont des conditions déterminantes de votre droit d'utiliser le Service[1]. »

On peut obtenir une adresse webmail en quelques minutes seulement. Il suffit de se connecter à la page d'accueil d'un de ces fournisseurs, de suivre les instructions, de sélectionner le bon service et de fournir des informations personnelles peu ou pas contrôlées. L'adresse e-mail ainsi que l'espace de stockage sont quasiment attribués en temps réel, et l'adresse est immédiatement opérationnelle.

1. Conditions d'utilisation des services Yahoo ! France (septembre 2007).

Lorsque les informations personnelles données par l'utilisateur sont inexactes, celui-ci peut considérer qu'il peut naviguer et interagir au moyen de cette adresse e-mail de manière anonyme.

5. Accéder à Internet à partir d'un accès public

Au premier trimestre de 2006, le Forum des droits sur l'Internet [1] évaluait à trois mille le nombre de points d'accès publics à Internet en France. Cybercafés, bibliothèques, jardins publics dans les grandes villes : les accès publics se multiplient, et c'est par millions que les internautes se connectent désormais à Internet par ce biais.

À la différence des accès individuels, réservés aux abonnés identifiés, les accès publics sont ouverts à tous, généralement sans identification préalable.

6. Utiliser un anonymiseur

Le moyen le plus sophistiqué pour obtenir l'anonymat est de passer par des sites dits « anonymiseurs ». Le but de ces sites est de faire échec au système d'identification par adresse IP. Il s'agit de permettre à l'internaute d'utiliser un serveur « mandataire » (*proxy* en anglais) afin de constituer un relais intermédiaire entre lui et le service Internet qu'il souhaite utiliser. Le service Internet destinataire reçoit les requêtes par le biais du serveur mandataire et ne dispose dès lors que de l'adresse IP de ce dernier.

Le site *anonymouse.org* fournit un service gratuit d'anonymisation de la navigation Web.

Les figures 2.1 à 2.3 illustrent l'utilisation d'un anonymiseur.

1. Association créée à l'initiative du gouvernement Jospin le 14 mars 2006 *(www.foruminternet.org)*.

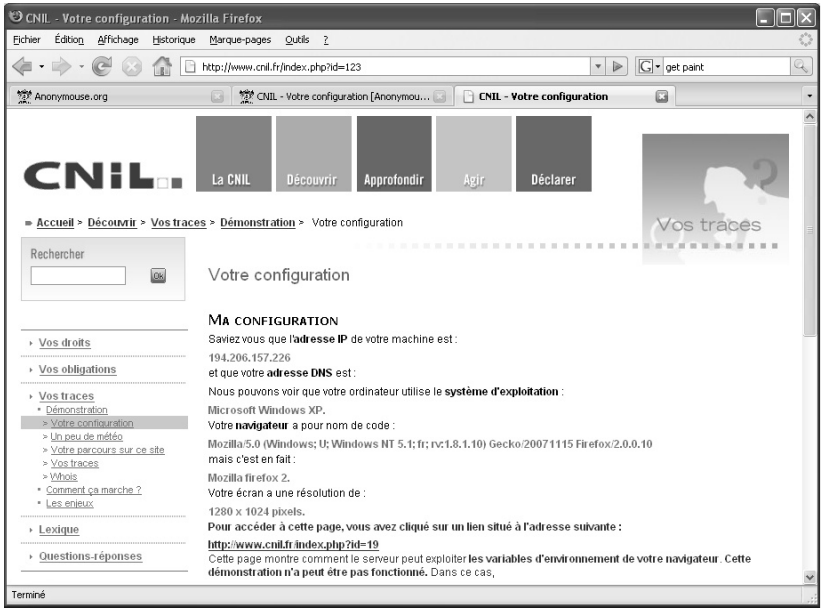

Figure 2.1 – Informations de traçabilité de l'adresse IP et de la configuration d'un ordinateur connecté au site de la CNIL (*www.cnil.fr*)

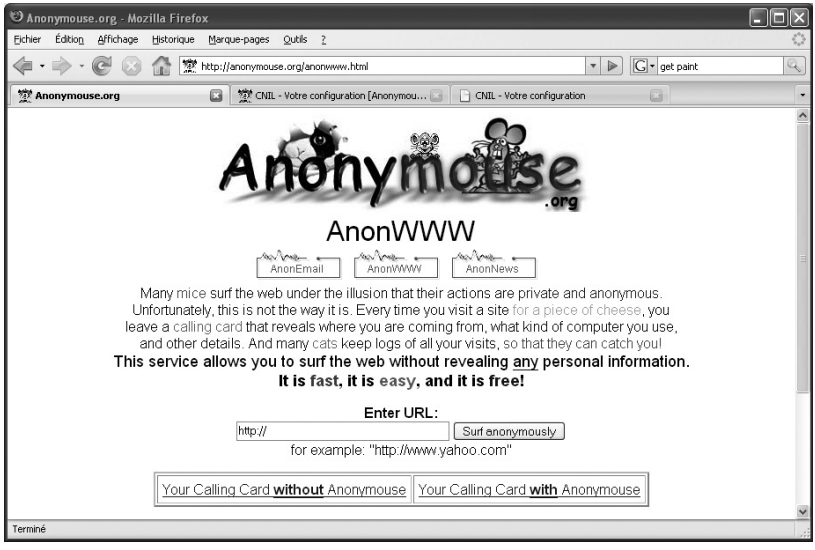

Figure 2.2 – Processus d'anonymisation du site anonymouse.org

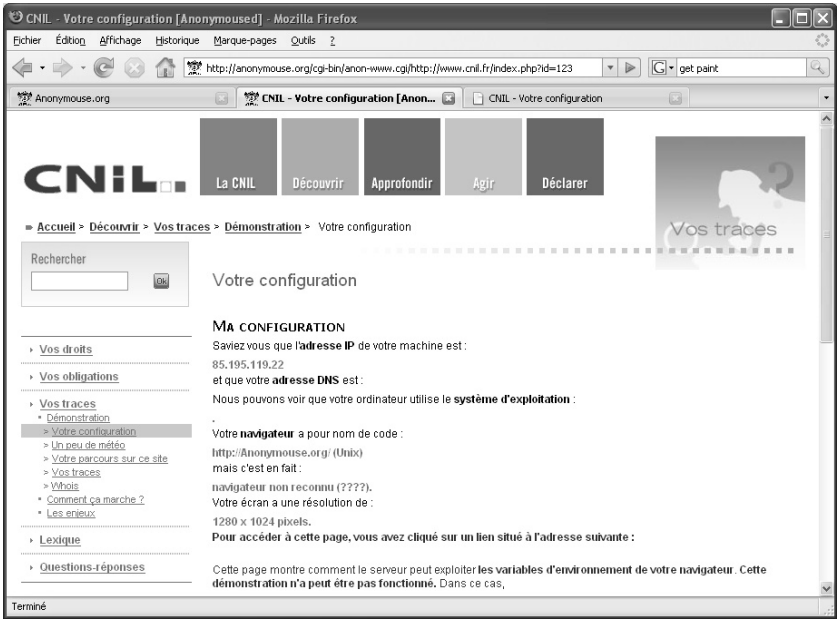

Figure 2.3 – Informations de traçabilité fournies par la CNIL après anonymisation de la navigation

Des services commerciaux tels que anonymizer. com confèrent *une anonymisation plus ou moins efficace. Si la plupart d'entre eux permettent à l'utilisateur de se présenter comme un internaute auquel est affectée l'adresse IP du proxy, certains d'entre eux véhiculent dans des en-têtes supplémentaires (notamment le champ* HTTP_X_FORWARDED_FOR) des informations qu'ils relayent relatives à l'adresse IP réelle du demandeur. Le chaînage de plusieurs de ces systèmes permet de renforcer l'anonymisation, un proxy étant chaîné à un ou plusieurs autres proxy.

D'autres services, appelés « remailers », permettent une anonymisation de l'envoi des e-mails en retirant de leurs en-têtes les informations permettant d'en identifier l'expéditeur.

Enfin, certains outils d'anonymisation en peer-to-peer, tels que TOR (The Onion Router), Freenet ou GNUnet, mettent en œuvre un routage anonymisé et chiffré. Seule l'adresse IP du dernier pair est révélée au destinataire final, les pairs intermédiaires se contentant de relayer les

requêtes chiffrées, donc inintelligibles, au pair le plus proche, et ainsi de suite. Il est dès lors très difficile de remonter la chaîne des pairs jusqu'à l'initiateur de la requête. Le problème principal de ce type de service est sa lenteur, puisque la requête doit être relayée *n* fois avant d'arriver à bon port.

7. Chiffrer (crypter) les communications

Selon la définition donnée par l'article 29 de la LCEN[1], on appelle cryptologie toute technique matérielle ou logicielle permettant de transformer des données, qu'il s'agisse d'informations ou de signaux, à l'aide de conventions secrètes ou pour réaliser l'opération inverse, avec ou sans convention secrète.

Le fait de transformer une information claire au moyen de conventions secrètes (cryptographie symétrique) privées ou publiques (cryptographie asymétrique), afin de ne pas la rendre accessible au public et/ou pour en garantir l'authenticité, constitue un acte de cryptologie.

Pendant très longtemps, la cryptologie a été considérée comme une arme de guerre. Son statut a ensuite évolué, d'abord en 1990 puis en 1996, à l'occasion de différentes lois de libéralisation du secteur des télécommunications[2]. Le régime de la cryptologie est aujourd'hui quasi libéralisé.

Les e-mails envoyés en clair sur les réseaux sont susceptibles d'être interceptés. La cryptographie permet de réserver la lecture des e-mails aux seuls destinataires choisis par l'expéditeur. Il est recommandé de chiffrer (crypter) également les fichiers attachés aux e-mails.

Vers un droit à l'anonymat ?

Les partisans de l'anonymat dans les réseaux numériques souhaitent qu'il soit protégé par la loi ou, à tout le moins, qu'il ne soit pas interdit. Ils font valoir à ce titre plusieurs arguments.

1. Loi n° 2004-575 du 21 juin 2004, dite Loi pour la confiance dans l'économie numérique.
2. Loi n° 90-1170 du 29 décembre 1990 sur la réglementation des télécommunications et loi n° 96-659 du 26 juillet 1996 de réglementation des télécommunications.

D'abord, l'anonymat répond à la volonté déclarée des citoyens de ne pas laisser leurs données à caractère personnel en libre accès, au risque de les voir happées par de gigantesques bases de données, à commencer par celles des moteurs de recherche de type Google. Il est incontestable que nos données à caractère personnel sont devenues l'enjeu d'une marchandisation de grande ampleur. La face immergée de l'iceberg est le Spam, ou message non sollicité, ces centaines d'e-mails qui polluent nos boîtes à lettres électroniques.

La collecte d'adresses électroniques est le préalable nécessaire à ces agissements, laquelle collecte se fait le plus souvent de manière illicite, sans notre accord préalable. Laisser notre adresse e-mail sur un forum de discussion, signer une contribution sur un blog, acheter un nom de domaine et une ou plusieurs adresses e-mail associées nous font courir le risque de voir notre adresse aspirée et, par voie de conséquence, notre boîte à lettres électroniques déborder de messages non sollicités. L'anonymat est la meilleure défense contre de telles pratiques.

Ceux qu'on commence à appeler les « marchands de vie privée » peuvent toutefois se montrer plus subtils. Ils nous observent lorsque nous naviguons sur Internet. Les moyens qu'ils utilisent pour cela sont multiples. Ils vont du cookie[1] à des techniques permettant d'identifier la langue utilisée par le navigateur du visiteur, le pays à partir duquel celui-ci s'est connecté, voire l'adresse IP utilisée, les habitudes de connexion, d'achat, etc. Ces informations ont beau être partielles, puisque couplées à une identification, elles n'en ont pas moins une forte valeur marchande,

1. Voici la définition qu'en donne l'encyclopédie en ligne Wikipédia : « Les cookies sont de petits fichiers texte stockés par le navigateur Web sur le disque dur du visiteur d'un site Web qui servent (entre autres) à enregistrer des informations sur le visiteur ou sur son parcours dans le site. Le webmestre peut ainsi reconnaître les habitudes d'un visiteur et personnaliser la présentation de son site pour chaque visiteur ; les cookies permettent alors de garder en mémoire combien d'articles il faut afficher en page d'accueil ou encore de retenir les identifiants de connexion à une éventuelle partie privée : lorsque le visiteur revient sur le site, il ne lui est plus nécessaire de taper son nom et son mot de passe pour se faire reconnaître, puisqu'ils sont automatiquement envoyés par le cookie. »

car elles permettent d'établir un profil de consommation qui intéresse les professionnels du marketing[1]. Là encore, la seule solution pour lutter contre ces pratiques est l'anonymat, et c'est pourquoi il doit être préservé et protégé par la loi.

Un autre argument avancé par les défenseurs de l'anonymat sur Internet tient au syndrome *Big Brother*. Ce n'est plus le démarchage commercial non sollicité qui est en cause ici, mais la peur du contrôle. Pour contrôler une population entière, il faut d'abord identifier qui fait quoi et où. Cette volonté de contrôle est évidente dans les États non démocratiques. Mais même dans une démocratie, les citoyens peuvent faire l'objet de pressions ou d'intimidations.

Protégé par l'anonymat, un citoyen « anonyme » doit pouvoir exprimer sans crainte ses positions, tout en étant à l'abri de pressions, parfois même de poursuites judiciaires initiées dans le seul but de le faire taire. C'était l'argument avancé par le site Internet Ubifree pour justifier l'anonymat de ses contributeurs. S'ils avaient été identifiés, ceux-ci auraient pu encourir la sanction de leur employeur. L'association Reporters sans frontières[2] recommande ainsi expressément le recours à l'anonymat pour la mise en œuvre de blogs dans les pays où la liberté d'expression n'est pas garantie afin d'échapper à la censure et à la répression.

Certains vont plus loin et revendiquent pour l'anonymat le statut de droit constitutionnel. Aux États-Unis, un fort courant universitaire appelle à faire reconnaître le droit à l'anonymat par la Constitution[3], au même titre que la liberté de pensée et d'expression. Le professeur Lawrence Lessig, de la Harvard Law School de Boston, prétend quant à lui que la suppression de l'anonymat porterait atteinte aux principes d'égalité de

1. Arnaud Belleil, *E-Privacy, le marché des données personnelles : protection de la vie privée à l'âge d'Internet*, Dunod, 2001.
2. Reporters sans frontières, *Guide pratique du blogger et du cyberdissident*, 2004 (disponible en PDF sur le site de l'association, à l'adresse *www.rsf.org*).
3. Julie E. Cohen, « A Right to Read Anonymously : a Closer Look at Copyright Management in Cyberspace », *Connecticut Law Review,* n° 28, 1996.

la société. L'identification préalable des internautes amènerait les différents services du réseau à distinguer et même à discriminer entre ceux qui les intéressent, c'est-à-dire ceux à fort pouvoir d'achat, systématiquement favorisés, et les autres.

Quand les grandes marques jouent l'anonymat

Le marketing invisible, ou furtif (*stealth marketing*), est une nouvelle technique consistant, pour des agences de publicité, à s'introduire dans des forums, à créer des blogs, etc., pour le compte de marques, sans jamais révéler leur véritable dessein. Elles établissent ainsi une relation avec des internautes pour les pousser à l'achat sous couvert d'un discours bien évidemment favorable à la marque. « Nous n'essayons pas de censurer la critique, mais plutôt de la diluer dans un flot de buzz positif », a déclaré François Collet, responsable de l'agence Heaven, qui déclare être intervenu de cette manière pour la XBox de Microsoft[1].

Du côté des opposants à l'anonymat sur Internet, on invoque d'abord ses limites. Les boutiques en ligne, par exemple, en tant que commerce à distance, requièrent une identification préalable. Généraliser l'anonymat et l'ériger en droit serait, selon eux, condamner les achats sur Internet, alors qu'ils constituent l'un des principaux facteurs de diffusion de l'accès au réseau au plus grand nombre.

La criminalité et le terrorisme sont d'autres limites évidentes à l'anonymat. Pour les services de police et de justice, l'anonymat sur Internet et la volatilité des informations numériques sont des écueils majeurs.

Les détracteurs de l'anonymat dénoncent en outre la possibilité offerte ainsi aux internautes d'assouvir leurs fantasmes les plus sombres. La liberté qui leur est donnée étant sans limite, elle peut encourager et faciliter les comportements déviants, inciviques, voire délictueux ou criminels.

Enfin, l'anonymat est souvent associé par ses opposants à la délation et aux attaques personnelles, à la manière des « lettres anonymes », et rime avec irresponsabilité et lâcheté.

1. Yves Eudes, *Le Monde*, 1er février 2005, cité par Viviane Mahler, *Souriez, vous êtes ciblés*, Albin Michel, 2007.

La position de la loi

Disons-le sans détour : l'anonymat sur les réseaux n'est pas hors la loi, à condition qu'il ne serve pas de support à des activités illicites. Par exemple, le délit d'escroquerie est défini par l'article 313-1 du Code pénal comme « le fait, soit par l'usage d'un faux nom ou d'une fausse qualité, soit par l'abus d'une qualité vraie, soit par l'emploi de manœuvres frauduleuses, de tromper une personne physique ou morale et de la déterminer ainsi, à son préjudice ou au préjudice d'un tiers, à remettre des fonds, des valeurs ou un bien quelconque, à fournir un service ou à consentir un acte opérant obligation ou décharge ». Le recours à l'anonymat peut soutenir de telles « manœuvres frauduleuses », caractérisant le délit d'escroquerie, si la recherche de l'anonymat visait intentionnellement à commettre un délit.

Cela dit, aucun texte de loi ne condamne par avance l'anonymat. Il n'existe pas non plus de texte de loi lui reconnaissant expressément une validité juridique. Ni condamné, ni reconnu, l'anonymat vit donc en droit dans une sorte de clandestinité. En l'absence de texte répressif, on pourrait certes estimer que l'anonymat est légal en droit français, mais, comme nous allons le voir, l'absence de reconnaissance explicite engendre des hésitations législatives fluctuant au gré des contextes et des époques.

On peut observer deux grands mouvements juridiques contradictoires. L'un considère l'anonymat comme le garant de la protection des libertés individuelles et du respect de la vie privée. Cet esprit se retrouve dans la loi informatique et libertés de 1978[1], dont l'article 28 prévoit que « toute personne physique a le droit de s'opposer, pour des motifs légitimes, à ce que des données à caractère personnel la concernant fassent l'objet d'un traitement ». La notion de « motifs légitimes » a été abondamment commentée[2] et analysée par les tribunaux. Tous

1. Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel.
2. André de Laubadère, *Loi relative à l'informatique, aux fichiers et aux libertés*, AJDA, 1978 ; Xavier Linant de Bellefonds, Alain Hollande, *Pratique du droit de l'informatique*, Delmas, 2002.

considèrent qu'elle s'apprécie au cas par cas mais peut parfaitement recouvrir la volonté d'une personne qu'on respecte sa vie privée.

Certaines législations spécifiques protègent expressément l'anonymat. Tel est le cas du Code de la propriété intellectuelle, qui prévoit le cas des œuvres anonymes. L'article L113-6 de ce code prévoit ainsi que c'est l'éditeur ou le producteur qui représente l'auteur anonyme, tant que celui-ci n'a pas déclaré son identité. Le code prévoit d'ailleurs dans ce cas une durée de protection spécifique de soixante-dix ans après première publication d'une œuvre et non de soixante-dix ans après la date de décès de l'auteur, laquelle n'est pas connue.

Le second mouvement législatif et jurisprudentiel opposé à l'anonymat a pris de l'ampleur dans la période récente grâce ou à cause d'Internet. Il s'est notamment signalé en France avec l'arrêt altern.org/Estelle H. du 10 février 1999[1]. Altern.org était un hébergeur gratuit qui avait pris le parti d'accepter des hébergements sans identifier ses clients. Mademoiselle Estelle H., à l'époque épouse bien connue d'un grand chanteur français, se plaignait que sept photos privées la représentant étaient hébergées par altern.org. Ce dernier n'était ni l'auteur des clichés, ni l'éditeur des pages.

La cour d'appel a pourtant retenu à son encontre « qu'en offrant, comme en l'espèce, d'héberger et en hébergeant de façon anonyme, sur le site altern.org qu'il a créé et qu'il gère, toute personne qui, sous quelque dénomination que ce soit, en fait la demande aux fins de mise à disposition du public ou de catégories de publics, de signes ou de signaux, d'écrits, d'images, de sons ou de messages de toute nature qui n'ont pas le caractère de correspondances privées, altern.org excède manifestement le rôle technique d'un simple transmetteur d'informations et doit, d'évidence, assumer à l'égard des tiers aux droits desquels il serait porté atteinte dans de telles circonstances, les conséquences d'une activité qu'il a, de propos délibérés, entrepris d'exercer dans les conditions susvisées ».

Altern.org a été condamné à près de 50 000 euros de dommages et intérêts (300 000 francs à titre principal), ce qui constituait un très lourd quantum

1. CA de Paris, arrêt du 10 février 1999, Estelle H./Valentin (*www.legalis.net*).

pour quelques photos privées et un hébergement gratuit. Il est évident que le recours à une prestation anonyme a fortement et négativement influencé la cour.

La volonté de lutter (sans le dire) contre l'anonymat se retrouve dans la législation européenne, qui impose l'obligation d'identification au commerçant électronique et au responsable de la publication d'une communication publique par voie électronique, autrement dit tout site Web, page personnelle ou blog.

Le statut du commerce électronique est encadré par une directive communautaire du 8 juin 2000[1], qui institue au sein du marché intérieur européen un cadre garantissant la sécurité juridique et la transparence du commerce électronique pour les entreprises ainsi que pour les consommateurs. En France, ces dispositions ont été transposées dans la LCEN le 21 juin 2004[2], qui définit le commerce électronique comme « l'activité économique par laquelle une personne propose ou assure à distance et par voie électronique la fourniture de biens ou de services ». L'article 19 de cette loi impose au cybercommerçant des obligations d'identification et de transparence et le place en situation d'illégalité s'il ne s'identifie pas selon les critères imposés. L'anonymat devient donc hors la loi dans ces cas précis.

Les mentions obligatoires d'identification sont la raison sociale ou les nom et prénoms des commerçants personnes physiques, leur lieu d'établissement, leur adresse de courrier électronique, ainsi que leurs coordonnées téléphoniques, leur numéro d'inscription au registre du commerce ou au registre des métiers, leur capital social, l'adresse de leur siège social, leur numéro de TVA intracommunautaire et enfin, le cas échéant, l'autorité à laquelle leur activité est soumise s'il s'agit d'une activité réglementée.

Malgré ces obligations légales, nombreux sont les commerçants sur Internet qui persistent à rester dans l'anonymat, soit par volonté, soit par

1. 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.
2. Loi n° 2004-575 du 21 juin 2004, dite loi pour la confiance dans l'économie numérique (LCEN).

ignorance de la loi. Le rapport de la DGCCRF (Direction générale de la concurrence de la consommation et de la répression des fraudes) de 2006 fait un constat révélateur concernant ces mentions obligatoires[1]. Sur un total de 5 038 opérations de contrôle effectuées en 2006, la DGCCRF a constaté qu'un tiers des sociétés contrôlées se trouvaient en infraction pour certaines mentions obligatoires. Les secteurs les plus surveillés sont les loteries et concours, les sonneries téléphoniques et l'hôtellerie en ligne. Après contrôle, près de 90 % des entreprises se seraient mises en conformité avec la loi.

Selon ces mêmes dispositions, le commerçant sur Internet doit permettre un « accès facile, direct et permanent utilisant un standard ouvert[2] ». La mention « standard ouvert » a pour objet d'éviter que l'utilisateur soit contraint d'acquérir des logiciels spécifiques pour accéder à des informations obligatoires. *A priori*, un lien hypertexte sur la page d'accueil suffirait à satisfaire cette obligation[3].

D'autres dispositions légales destinées à lutter contre l'anonymat sont insérées dans la LCEN du 21 juin 2004. Elles ont trait au « droit de la presse » et concernent tous les sites Web, dont les responsables deviennent, au regard de la loi et par la seule mise à disposition du public des contenus de leur site, des directeurs de publication.

La loi distingue selon que l'éditeur du site est un professionnel ou non. Un éditeur est considéré comme professionnel dès lors que « son activité est d'éditer un service de communication au public en ligne ». S'agissant de l'éditeur non professionnel, la loi le soumet à des obligations de déclaration minorées. Fait remarquable et symptomatique, la loi reconnaît à cet éditeur non professionnel le droit de « préserver son anonymat », tout en le soumettant à des obligations de déclaration[4].

Le tableau 2.1 récapitule les obligations des uns et des autres en matière d'identification.

1. Bilan 2006 du réseau de surveillance Internet de la DGCCRF disponible à l'adresse *http://www.minefi.gouv.fr/directions_services/dgccrf.*
2. Art. 19 de la LCEN.
3. Christiane Féral-Schuhl, *Journal du Net*, 15 décembre 2004.
4. Art. 6, III, 2 de la LCEN.

Tableau 2.1 – Obligations d'identification des éditeurs de site Web

Situation juridique	Obligations de mise à disposition[a]
Éditeur personne physique professionnel (article 6.III.1a LCEN)	– Nom – Prénom – Domicile – Numéro de téléphone – Numéro d'inscription au RCS ou au registre des métiers – Noms des directeur, codirecteur de publication et responsable de la rédaction – Nom, dénomination ou raison sociale et numéro de téléphone de l'hébergeur
Éditeur personne morale professionnel (article 6.III.1b LCEN)	– Dénomination ou raison sociale – Siège social – Numéro de téléphone – Numéro d'inscription au RCS ou au registre des métiers – Capital social – Adresse – Noms des directeur, codirecteur de publication et responsable de la rédaction – Nom, dénomination ou raison sociale et numéro de téléphone de l'hébergeur
Éditeur non professionnel (article 6.III.2 LCEN)	Nom, dénomination ou raison sociale et adresse de l'hébergeur, sous réserve de lui avoir communiqué tous les éléments d'identification personnelle prévus ci-avant pour l'éditeur personne physique professionnel

a. Décret n° 2007-750 du 9 mai 2007, qui ajoute l'obligation de mettre en ligne le numéro Siren pour les entreprises.

L'indication de ces mentions obligatoires a pour objectif principal de permettre aux tiers d'exercer un droit de réponse ou de notifier la mise en ligne d'un contenu illicite.

Certains auteurs ont dénoncé la quasi-inexistence de sanctions en cas de non-respect des obligations d'identification[1]. En réalité, le manquement à ces obligations est puni d'une amende pouvant aller jusqu'à 750 euros par infraction constatée (contravention de 4e classe)[2]. De plus,

1. Cédric Manara, « Mentions légales d'un site Web, gare aux contraventions », *Journal du Net*, 21 mai 2007.
2. Art. 131-13 du Code pénal et R.123-237 du Code du commerce.

et surtout, si cette obligation d'identification fait défaut et que cette absence crée un préjudice à une personne en particulier, tel que l'impossibilité de faire jouer un recours, la victime peut en obtenir réparation en justice.

Un anonymat bien tempéré

Au regard des textes et de la jurisprudence, l'anonymat sur les réseaux numériques doit être tempéré pour au moins deux motifs.

L'immense majorité des internautes souscrit un abonnement auprès d'un fournisseur d'accès, ou FAI, pour accéder au réseau. Il en va de même pour la téléphonie mobile. Les FAI et opérateurs ont l'obligation de se déclarer auprès de l'Arcep (Autorité de régulation des communications électroniques et des postes).

L'article L33-1 du CPCE (Code des postes et des communications électroniques) dispose que « l'établissement et l'exploitation des réseaux ouverts au public et la fourniture au public de services de communications électroniques sont libres sous réserve d'une déclaration préalable auprès de l'Autorité de régulation des communications électroniques et des postes ». Le même code prévoit que le défaut de déclaration est puni de peines maximales d'un an d'emprisonnement et de 75 000 euros d'amende.

Les opérateurs sont donc clairement recensés et identifiés. Ils sont liés à leurs clients par contrat, et les clients sont identifiés avec certitude, ne serait-ce que pour des questions de paiement. Un FAI attribue à chaque client des données techniques de connexion nominatives (ligne téléphonique, compte, etc.). À chaque connexion, les serveurs du FAI attribuent automatiquement au client une adresse IP parmi la plage d'adresses IP qui lui ont été attribuées. Avec cette adresse IP, le client signe chacune de ses interactions sur le réseau Internet. Comme on le voit, on est très loin de l'anonymat…

Le législateur a parfaitement compris cette dimension technique puisqu'il l'a intégrée à sa façon dans la loi. Prenant acte de l'impossibilité d'imposer, sauf à des personnes ayant à un moment donné un statut particulier sur Internet, l'identification préalable, il a imposé, dans des cas qui sont

loin d'être définis avec précision, la collecte obligatoire des données techniques de connexion aux opérateurs[1] et à toute personne « dont l'activité est d'offrir un accès à des services de communication au public en ligne » et à celles qui « assurent, même à titre gratuit, pour mise à disposition du public par des services de communication au public en ligne », l'obligation de détenir et conserver « les données de nature à permettre l'identification de quiconque a contribué à la création du contenu ou de l'un des contenus des services dont elles sont prestataires »[2].

BNP Paribas a été condamnée par la cour d'appel de Paris[3] pour n'avoir pu produire de telles données de connexion en justice, les juges considérant que la banque donnait accès à Internet à ses salariés et était donc redevable de cette obligation. S'ils confirment cette jurisprudence, les tribunaux auront définitivement condamné l'anonymat sur les réseaux numériques, imposant à toutes les organisations, entreprises et administrations de surveiller et collecter les données de toutes personnes auxquelles elles donnent accès au réseau.

En conclusion

L'anonymat sur les réseaux numériques vit au moins trois paradoxes :

- Internet, le premier de ces réseaux, a été conçu pour préserver l'anonymat. C'est là une des explications de son succès. Pourtant, jamais citoyens, utilisateurs, consommateurs, salariés n'auront été autant traqués du fait des moyens que ce réseau procure en termes de traçabilité.
- À ce jour, l'anonymat est un moyen de défense efficace du citoyen contre la marchandisation et le contrôle de la vie privée. Pourtant, la loi, expression de l'intérêt général, sans rendre illégale la pratique de l'anonymat, la pourchasse en secret. Le législateur impose en effet aux opérateurs et à toutes les organisations donnant accès au réseau

1. Art. L34-1 du Code des postes et des communications électroniques et décret n° 2006-358 du 24 mars 2006 relatif à la conservation des données des communications électroniques.
2. Loi n° 2004-575 du 21 juin 2004 (LCEN).
3. CA de Paris, 4 février 2005, arrêt publié en intégralité sur le site du Forum des droits sur l'Internet *(www.foruminternet.org).*

ou stockant des données de surveiller, tracer et conserver toutes les données d'identification. Compte tenu de cette obligation d'identification sous peine de sanctions pénales, les acteurs professionnels s'organisent pour tracer les flux. De ce fait, ils organisent la lutte contre l'anonymat.

- L'anonymat n'a pas de statut juridique. Cette situation crée une ambiguïté que l'on retrouve jusque dans la « Nétiquette », ces règles de bonne conduite sans valeur juridique, conçues à l'origine essentiellement pour les groupes de discussion ou newsgroup[1]. L'article 3.1.1 fixant les règles générales pour les listes de diffusion stipule que « les postages *via* des serveurs d'anonymat sont acceptés dans certains groupes de nouvelles et désapprouvés dans d'autres ». On ne saurait être moins précis…

Le droit français ne pourra se passer longtemps d'affirmer clairement sa doctrine sur la légalité ou non de l'anonymat. Cette question fondamentale gît au cœur de toutes les problématiques de la société de l'information (droit d'auteur, vie privée, etc.). Elle pourrait bien devenir demain le pivot de nos libertés individuelles et collectives.

Si le droit à l'anonymat n'est pas absent de la loi informatique et libertés, il n'est pas pour autant clairement affirmé. Pour notre part, nous militons pour que l'anonymat soit élevé au rang de droit constitutionnel, de droit de l'homme. Un tel droit devrait, par exemple, imposer l'anonymisation par défaut ou l'obligation pour les fournisseurs d'accès de conserver anonyme toute donnée collectée.

Le commerce n'a rien à craindre de cette évolution. Il devra simplement organiser un marché de l'identification pour rendre des services ou vendre des produits. Quant aux autorités publiques, elles ne devraient rien avoir à craindre non plus de cette situation. L'anonymat pourrait être levé dans des circonstances particulières et sous le contrôle d'un juge, seul capable de vérifier l'usage non abusif de toute demande tendant à lever un anonymat.

Finalement, le droit à l'anonymat n'est-il pas le meilleur atout pour que la confiance s'installe durablement dans les réseaux numériques ?

1. RFC 1855, « Netiquette Guidelines », traduite par Jean-Pierre Kuypers.