Internet et identité virtuelle des personnes

Philippe Mouron

INTERNET ET IDENTITÉ VIRTUELLE DES PERSONNES

Par

Philippe Mouron
Allocataire-Moniteur à l'IREDIC
Université Paul Cézanne – Aix-Marseille III

L'interconnexion mondiale des ordinateurs et la masse croissante des données numériques échangées sur les réseaux ont donné naissance à un nouvel espace de communication et d'information : le cyberespace.

Pure fiction il y a encore peu de temps[1], cet espace nouveau est devenu une réalité, paradoxalement caractérisée par sa "virtualité". Dans son sillage, le préfixe "cyber" est venu accompagner un grand nombre de termes, dont l'objet se trouve peu ou prou lié à cet espace, en tant qu'entité technique. Dans le domaine juridique, on parle déjà d'une "cyberjustice", dont le ressort constitue le principal sujet de discussion[2]. De manière générale, le terme de "cyberculture" a été proposé pour qualifier d'un point de vue sociologique les pratiques, attitudes et modes de pensée induits par le cyberespace[3]. Ceux-ci sont très nombreux et diversifiés, allant du simple service de messagerie jusqu'à la (re)constitution d'univers virtuels autonomes et persistants[4], en passant par le phénomène des pages personnelles ou encore le commerce électronique. Leur utilité est aussi très hétérogène : achat, vente, communication, information, discussion, partage et/ou échange de fichiers, distraction, jeu… voire même vivre une seconde vie ! Les caractéristiques spéciales du web 2.0, basé sur l'interactivité et la construction participative des réseaux, fournissent naturellement une très grande capacité de création aux internautes. La vie réelle semble d'une certaine façon se décliner dans le cyberespace.

Une problématique apparaît néanmoins : au même titre qu'un individu se projette dans l'espace réel, sa projection doit pouvoir être assurée dans le cyberespace. Il faut distinguer le corps et la personne. Comment l'identité de celle-ci sera-t-elle appréhendée dans un monde immatériel ? L'identité réelle est-elle transposable au monde virtuel ? Ces questions attirent l'attention sur ce que pourrait être l'identité virtuelle. L'emploi de cette expression résume efficacement ce dont il est question. Il s'agit bien de savoir ce qu'est l'"identité" (prise en tant qu'ensemble des éléments de fait et de droit qui

---

[1] La paternité de ce néologisme (contraction des termes "cybernétique" et "espace") est attribuée à l'écrivain William Gibson, précisément dans son roman *Neuromancien*, paru en 1984.
[2] CHABOT G., "La cyberjustice : réalité ou fiction ?", *D.*, 2003, Chronique, pp. 2322-2325.
[3] LÉVY P., *Cyberculture – Rapport au Conseil de l'Europe*, Éd. Odile Jacob, Paris, 1997, p. 17.
[4] Ces univers sont souvent le support de jeux pouvant impliquer plusieurs millions de personnes ; ils sont communément appelés les "jeux de rôle en ligne massivement multijoueur".

permettent de singulariser quelqu'un) dans une dimension "virtuelle" (c'est-à-dire dans un espace immatériel distinct de la réalité concrète). La distinction établie avec l'identité réelle permet de remonter jusqu'à la notion d'"identité personnelle", juridiquement très floue, proche de l'intégrité morale, mais dont l'unicité semblait pourtant admise depuis longtemps[5]. Schématiquement, il s'agit de l'identification (nom, prénom, adresse…) et de la personnalité ; les données "identifiantes" comprennent celles de l'état civil, mais aussi les choix culturels, politiques, sexuels, religieux[6]… sans oublier les données biométriques, et bientôt de nouveaux identifiants, à l'utilité discutable, comme les étiquettes RFID sous-cutanées.

Le dédoublement opéré par le cyberespace vient bouleverser la donne. Si l'étymologie latine du terme "identité" renvoie au "caractère de deux objets identiques", il n'est pas certain que l'identité d'une personne soit la même dans le monde réel et dans le cyberespace. Ce dernier est en effet caractérisé par deux principes essentiels : la publicité et la liberté. Le caractère éminemment public de l'Internet assure ainsi une totale liberté d'accès aux données d'identité qui sont divulguées par les personnes. Elles peuvent être utilisées notamment à des fins économiques, comme c'est le cas au niveau du commerce électronique. Par ailleurs, la liberté, garantie par la technique, assure aux internautes le choix de leur identité et la maîtrise de sa substance. L'individu se trouve donc divisé en une multitude d'informations, dont il ne maîtrise plus la circulation une fois qu'elles sont divulguées. L'identité est elle-même éclatée en plusieurs dimensions assurant une ubiquité fonctionnelle de la personne dans le cyberespace[7].

Ces caractéristiques de l'identité virtuelle bouleversent un grand nombre d'institutions établies par le Droit. L'intégrité de la personne, la permanence et l'unicité du corps sont remises en cause au profit d'informations fragmentaires, éparpillées, et dont la véracité ne peut être vérifiée. Le nom, jusque là subi, peut être choisi. Par conséquent, le consentement peut être donné sous un faux nom. La volonté exprimée par un acte juridique ne sera peut-être pas celle de la personne sous le nom de laquelle il est passé. De même que l'engagement de la responsabilité pourra se heurter au voile d'une identité de dissimulation. L'usurpation est en effet rendue possible par la reprise libre des données. Elle dépassera la simple reprise du nom, et s'accompagnera souvent d'autres données identifiantes, comme l'image de la personne. Au-delà, leur utilisation peut encore donner lieu à la diffamation, l'injure, ou simplement la déformation de la réalité. De manière générale, la sécurité juridique est remise en cause, la confiance en l'économie numérique peine à s'affirmer.

---

[5] GUTMAN D., *Le sentiment d'identité – Étude de droit des personnes et de la famille*, LGDJ, Paris, 2000, pp. 1-8.

[6] BIOY X., "L'identité de la personne devant le Conseil Constitutionnel", *RFDC*, n° 65, janvier 2006, p. 74.

[7] FRAYSSINET J., "Droit, droits et nouvelles technologies", *Rapport présenté au 30ème Congrès de l'Institut International de Droit d'Expression et d'Inspiration Françaises*, Le Caire - décembre 2006, p. 4 (disponible sur le site de l'Iredic : http:/www.iredic.com).

Ces constats interpellent le juriste, et l'amènent à examiner de plus près l'identité virtuelle. Son lien avec l'identité réelle est totalement insaisissable, voire même indéfinissable, tant les potentialités sont nombreuses. Pourtant, cette caractéristique ne le rend pas inexistant. La technique assure avant tout un prolongement de l'identité réelle dans le monde virtuel. Ce n'est que ce prolongement qui est qualifiable d'identité virtuelle. Il convient alors de rechercher quels peuvent être ses éléments constitutifs. Si elle doit exister, comment le droit pourrait l'appréhender ? Quel en est le régime juridique ?

La réponse est multiple car la définition de l'identité virtuelle recouvre des données bien différentes. Mais elle est simple car le droit existant suffit pour les qualifier et en définir les régimes juridiques. En cela, le cyberespace n'est que le vecteur de comportements dont il ne détermine que le mode d'expression, sans le conditionner[8]. Cette étude a le mérite de révéler les évolutions de la notion d'identité personnelle, et de soulever la question d'un droit au respect de l'identité[9]. Encore faut-il déterminer quels types de données seraient concernés par ce droit. Une gradation peut être établie, allant de celles qui relèvent objectivement d'une personne réelle vers celles qui tendent à plus de virtualité. L'identité virtuelle recouvre ainsi les trois acceptions suivantes, présentées dans leur ordre logique :

- l'identité numérique ; il s'agit de la représentation technique de la personne et de ses actes dans le cyberespace ; elle est la plus proche de la personne réelle, traduisant ses actes en données numériques (adresse IP, données de connexion).

- l'identité "virtualisée" ; elle consiste en une projection de l'identité réelle dans le monde virtuel, assumée ou non par son titulaire. Elle est donc constituée de données identifiantes réelles (nom, prénom, âge, orientation sexuelle, opinions, centres d'intérêt…).

- l'identité immatérielle ; ici, l'identité virtuelle est volontairement sans rapport avec l'identité réelle. La virtualité est alors absolue. L'anonymat refoulé cède le pas à la dissimulation sur le réseau ; l'internaute bénéficie du confort d'une identité fabriquée de toutes pièces, frauduleuse ou idéalisée[10], telle celle de l'avatar de jeu vidéo.

À l'opposé de l'identité réelle unique, se trouve donc une identité virtuelle plurielle. Le lien entre ses trois dimensions est aisé à tracer. La première, l'identité numérique, constitue un prolongement technique de l'identité réelle. Mais ses éléments constitutifs peuvent faire l'objet d'une virtualisation indépendante de la volonté de son titulaire, grâce à des logiciels de traçabilité[11] ; ces derniers visent à reconstituer l'identité réelle de la personne sur la base des sites visités. À ce titre, ces mêmes éléments

---

[8] VIVANT M., "Cybermonde : Droit et droits des réseaux", *JCP-G*, 1996, I, p. 401.
[9] MARINO L., "Les nouveaux territoires des droits de la personnalité", *Gaz. Pal.*, 19 mai 2007, p. 1483.
[10] POUSSON D., "L'identité informatisée", *in L'identité de la personne humaine – Étude de droit français et de droit comparé* (ss la dir. de POUSSON PETIT J.), Bruylant, Bruxelles, 2002, p. 373.
[11] FRAYSSINET J., "La traçabilité des personnes sur l'internet", *Droit et Patrimoine*, n° 93, mai 2001, p. 76.

intègrent aussi la seconde dimension, l'identité virtualisée. Celle-ci comprend également des informations (textuelles ou visuelles) de l'identité réelle divulguées dans le cyberespace. De ce fait, l'identité virtualisé recouvre elle-même deux acceptions bien différentes : dans le premier cas, il s'agit d'un "potentiel" de l'identité réelle, un portrait robot déterminé par la technique ; dans le deuxième cas, il s'agit d'une transposition plus exacte, mais non totale, de l'identité réelle dans le monde virtuel. Dans les deux cas, nous pouvons affirmer le caractère très improbable de la virtualisation. Enfin, dans la continuité de ce processus apparaît l'identité immatérielle, qui tend à se détacher au maximum de l'identité réelle. En vérité, elle en reste dépendante, n'étant que le fruit de l'imagination d'une personne bien réelle.

Au-delà du travail de classification, il importe de relever que le Droit tend déjà à renforcer l'adéquation de l'identité virtuelle plurielle et de l'identité réelle unique. Un grand nombre de textes de droit interne, épars et variés, protègent en effet la personne contre toute utilisation non souhaitée de ses données. En droit européen, la Cour européenne des Droits de l'Homme a rattaché cette protection au respect de la vie privée tel que défini par l'article 8 de la Convention, dans un rapport essentiellement vertical[12]. De même, cette exigence fait l'objet d'un article spécifique de la Charte des Droits fondamentaux de l'Union européenne[13]. Ces dispositions sont vouées à s'enrichir, en vue de protéger toujours plus l'intégrité de l'identité personnelle, tant dans sa dimension réelle que dans sa dimension virtuelle. Il importe en effet d'affirmer l'existence d'un véritable *habeas data*, corollaire de l'*habeas corpus* du monde réel. Si un certain nombre de législations l'ont explicitement reconnu, notamment en Amérique Latine[14], l'étude du droit positif français à l'aune du droit communautaire permet d'en dégager les bases. Celles-ci, encore incomplètes, intègrent les trois dimensions de l'identité virtuelle.

Cette dernière constitue initialement un prolongement technique de l'identité réelle (I). Mais elle aboutit à en faire une copie servile (II), la transposition de la personne ne pouvant être totale. Dans les deux cas, il importe que l'individu conserve le contrôle de ses données virtuelles.

I. L'identité virtuelle, prolongement technique de l'identité réelle

En premier lieu, la projection de la personne dans le cyberespace s'effectue au moyen d'identifiants et de données numériques dites "de connexion".

---

[12] SUDRE F., *Droit européen et international des droits de l'homme*, 9ème éd., PUF, Paris, 2008, pp. 468-470.

[13] Art. 8: "Toute personne a droit à la protection des données à caractère personnel la concernant. Ces données doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi. Toute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification. Le respect de ces règles est soumis au contrôle d'une autorité indépendante."

[14] GUADAMUZ A., "Habeas Data vs. The European Data Protection Directive", *The Journal of Information, Law and Technology*, 7 novembre 2001, http://www2.warwick.ac.uk.

Leur utilité première est d'assurer la connexion technique de l'utilisateur au monde virtuel. Elles ont un caractère éminemment dynamique, et jouent une fonction d'identification de la personne ou, du moins, de l'ordinateur connecté. Il s'agit du lien le plus proche de la personne réelle, sans être le plus sûr. L'ensemble de ces données constitue l'identité numérique qui siège à côté de l'individu charnel[15]. Le droit applicable à la protection des données personnelles peut aider à cerner les composants de cette identité. Leur appréhension par le droit est fonction d'une certaine finalité : protection du consommateur, identification des auteurs d'une infraction (lutte contre la cybercriminalité, le téléchargement, le terrorisme…). Au travers des textes, nous en dégagerons les éléments constitutifs.

Nous distinguerons l'adresse IP (*Internet Protocol*), donnée d'identification liant les deux identités, réelle et virtuelle (A), des autres données de connexion (B). Dans les deux cas, il importera de démontrer comment le Droit les rattache à une identité réelle. Si l'adresse IP constitue la base de l'identité numérique, les données de connexion sont celle de l'identité virtualisée.

A. L'adresse Internet Protocol, donnée commune aux identités réelle et numérique

Longtemps ignorée par le Droit, l'adresse IP constitue l'identifiant technique de tout ordinateur hôte ou usager connecté aux réseaux. Les récents débats relatifs à la lutte contre le téléchargement l'ont révélée à la jurisprudence et la doctrine. Si sa fonction d'identification technique la rattache à l'identité numérique (1), il se pose la question de savoir s'il s'agit d'une donnée à caractère personnel, ce qui la rattacherait également à l'identité réelle (2).

1. L'adresse IP, base de l'identité numérique

L'organisation de l'Internet repose sur le Protocole Internet, qui détermine la communication des informations entre serveurs, sites et ordinateurs connectés[16] (a). L'adresse IP constitue le "seuil" du monde virtuel pour l'utilisateur (b).

a) L'adresse IP, protocole technique

Tout ordinateur est identifié par le protocole grâce à l'adresse IP. Sa fonction est avant tout technique, et ses caractéristiques la rendent inaccessible aux sens de l'être humain. Elle se présente comme une série de

---

[15] DUBUISSON E., "La personne virtuelle : propositions pour définir l'être juridique de l'individu dans un échange télématique", *DIT*, 1995/3, pp. 11 et 15.

[16] POSTEL J., *RFC: 791 Internet Protocol*. Traduction française de FRÉMAUX V. G., site de DIML : http://www.diml.org/

quatre groupes, composés chacun de un à trois chiffres, et séparés par des points. Initialement rattachée au nom de domaine[17], elle le transcende pourtant puisque tout ordinateur connecté reçoit une adresse IP, même celui d'un particulier. Elle peut être statique ou dynamique, changeant alors à chaque connexion. Cette deuxième solution est la plus fréquente, eu égard aux limites mathématiques de la série de chiffres. Attribuée par les fournisseurs d'accès à Internet (FAI), ceux-ci disposent d'un "pool" d'adresses IP, affectées pour des sessions d'utilisation bien précises, limitées dans le temps[18]. Quelles que soient ses caractéristiques, elle constitue la terminaison nécessaire d'une connexion, l'adresse d'envoi ou de réception des données numériques, la présence sur le réseau d'un ordinateur.

Son caractère technique en a fait initialement une donnée anonyme. La suite de chiffres précitée ne permet pas, par sa nature, d'identifier une personne. Elle n'identifie qu'un ordinateur, en lui attribuant une adresse de réception pour les informations. C'est là un point essentiel de la structure de l'Internet que le droit est venu stabiliser en consacrant un droit au secret[19], notamment à travers le principe de l'effacement des données de connexion. Nous y reviendrons par la suite. Notons toutefois que l'existence de ces données est conditionnée par celle de l'adresse IP, sans laquelle elles ne pourraient exister. La connexion trouve toujours sa source ou sa destination en un ordinateur particulier, qui doit être identifié. D'un point de vue à la fois plus humain et plus théorique, elle assure l'accès au cyberespace pour l'utilisateur de la machine.

b) L'adresse IP, ouverture sur le monde virtuel

Indépendamment de son caractère intrinsèquement anonyme, l'adresse IP est le fondement de l'identité virtuelle, entendue comme l'identité numérique, qui comprend l'ensemble des informations techniques caractérisant un utilisateur. Elle en constitue la base légitime, conditionnant l'existence sur le réseau.

Nous pouvons adopter un point de vue plus humain, en considérant que ces données elles-mêmes sont conditionnées par la volonté de l'homme-utilisateur. L'ordinateur n'est qu'un procédé technique au service de ce dernier ; il n'est pas connecté en permanence à Internet. L'adresse IP, qu'elle soit statique ou dynamique, n'existe pas de façon continue. Elle n'apparaît sur le réseau (dans le cyberespace) que pour une connexion bien particulière, voulue par l'utilisateur[20]. Sa mobilisation est fonction de la volonté de ce dernier. Il en est de même pour les données de connexion qui viendront se greffer dessus. L'ensemble ainsi constitué révèle les mouvements, les actions et les errements de l'internaute dans le cyberespace à travers les pages

[17] TRUDEL P., *Droit du cyberespace*, Éditions Thémis, Montréal, 1997, p. 17-1 et s.
[18] RENAULT F., "La panoplie technologique d'Internet au service ou au détriment de la liberté des individus ?", *in Le harcèlement numérique* (ss la dir. de GIROT J.-L.), Dalloz, Paris, 2005, p. 31.
[19] TRUDEL P., *op.cit.*, p. 11-59 et s.
[20] DUBUISSON E., *op. cit.*, p. 16.

visitées. En résumé, l'identité numérique est avant tout fonction de la volonté de l'homme. Elle représente même davantage la volonté que l'homme. Ce dernier, une fois né, ne peut décider de disparaître à sa guise ; l'adresse IP n'apparaît et ne disparaît que s'il le décide. Avec elle, c'est son existence dans le cyberespace qui est déterminée.

Ces développements nous amènent à un premier constat : si l'adresse IP constitue la base de l'identité numérique, son caractère anonyme permet de distinguer l'utilisateur réel et son double virtuel. Le second est commandé par la volonté du premier, mais sans faire apparaître son identité réelle. L'identité numérique pourrait se limiter à être une collection d'informations sans nom, et dont la cohérence serait d'être l'expression d'une seule et même volonté. Cela lui ôterait tout intérêt, notamment d'un point de vue juridique. En vérité, cet intérêt existe, tout simplement parce que le lien entre l'internaute réel et le clone virtuel n'est pas seulement subjectif.

L'identité numérique est aussi la projection objective d'une identité réelle. L'adresse IP en est le point de cristallisation. Si son caractère anonyme l'a longtemps cantonnée au rôle de simple procédé technique, le développement de la cyberculture a induit de nouvelles pratiques, et surtout de nouveaux abus. La répression ne pouvant se faire dans le cyberespace, c'est bien dans le monde réel qu'il est apparu nécessaire d'identifier les coupables. Derrière l'ordinateur, et l'adresse IP, c'est une personne bien réelle qui manipule les communications. L'identité virtuelle, dans toutes ses dimensions, n'est qu'une composante de l'identité personnelle d'un seul et même individu.

Mais comment faire le lien entre cet individu et l'identifiant numérique ? Le rôle de l'adresse IP pourrait-il dépasser le seul aspect technique ? Il importe d'envisager comment le droit s'en est emparé, révélant son appartenance à l'identité réelle des internautes.

2. *L'adresse IP, lien juridique entre l'identité réelle et l'identité numérique*

Le droit a longtemps ignoré l'adresse IP, aucun contentieux n'ayant été soulevé. Mais le développement du commerce électronique, du téléchargement illicite, de la cybercriminalité, ainsi que l'utilisation d'Internet par des réseaux terroristes ont attiré l'attention sur son statut juridique, spécialement sa qualité de donnée à caractère personnel (a). De fait, les débats ont révélé le lien qu'elle assure avec la réalité (b), ce qui permet d'envisager la qualification de domicile virtuel, commun aux deux identités (c).

a) L'adresse IP, donnée à caractère personnel ?

Un grand nombre de textes sont venus réglementer les nouvelles pratiques du cyberespace, avec l'objectif d'assurer l'identification des personnes dans le "monde réel". L'adresse IP accolée à un ordinateur peut identifier indirectement son propriétaire. Ses caractéristiques techniques localisent l'appareil et en déterminent le fournisseur d'accès. Le

rapprochement avec le fichier client détenu par ce dernier établit le lien avec ledit propriétaire. Cette brève analyse démontre déjà comment l'adresse IP intègre les deux identités, réelle et numérique. Si elle détermine techniquement la seconde, elle peut aussi être un élément d'identification de la première… du moins de l'ordinateur qu'elle a actionné. Le lien entre les deux reste relatif. Peut-on vraiment confirmer l'appartenance de l'adresse IP aux deux identités ? L'étude du droit applicable aux données personnelles nous éclaire sur la nature de ce lien.

L'état actuel du droit national et du droit communautaire permet de la qualifier de donnée à caractère personnel, voire même de donnée "indirectement" nominative. Pour la France, la loi Informatique et Libertés du 6 janvier 1978, modifiée par la loi du 6 août 2004, constitue le fondement du droit applicable aux données personnelles. S'il est regrettable qu'elle ne définisse pas explicitement l'adresse IP[21], ses dispositions permettent toutefois de la faire entrer dans le champ de ces données, en tant que "numéro d'identification"[22]. La même interprétation peut être retenue pour le droit communautaire, moins lacunaire sur la question. Ainsi, l'article 5 de la directive du 15 mars 2006, visant la conservation des données nécessaires pour identifier la source d'une communication sur Internet, inclut explicitement l'adresse IP. Selon l'article 2 de la même directive, elle peut faire figure de "donnée connexe" à l'identification de l'utilisateur. Celle-ci n'est en effet possible que si on la rapproche d'autres données.

Cette uniformité des textes n'est toutefois pas partagée par la jurisprudence. Des contentieux récents, relatifs à la lutte contre le téléchargement illicite, ont porté l'adresse IP devant les juges nationaux et communautaires. Face à la problématique de son statut juridique, deux solutions diamétralement opposées sont retenues : d'une part, l'adresse IP constituerait bien une donnée personnelle, car elle peut acquérir un caractère nominatif (selon une interprétation logique des textes) ; d'autre part, elle ne serait pas une donnée personnelle, car elle se limite à identifier un ordinateur, et permet au mieux de constater la matérialité d'une infraction[23]. On ne saurait nier que ces deux solutions sont parfaitement logiques, eu égard aux caractéristiques de l'adresse IP. L'enjeu de ces jurisprudences divergentes oppose la protection des données personnelles à celle des titulaires de droits

---

[21] FRAYSSINET J., "La loi relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi du 6 août 2004 : continuité et/ou rupture ?", *RLDI*, n° 9, octobre 2005, p. 51.
FRAYSSINET J., "Trente ans après, la loi "Informatique et libertés" se cherche encore", *RLDI*, n° 34, janvier 2008, p. 69.

[22] Art. 2 al. 2, loi 6 janvier 1978 : "Constitue une donnée à caractère personnel toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres.".

[23] Voir, entre autres : CA Paris, 15 mai 2007, *S. c./ Ministère Public et a.* et plus récemment CA Paris, 3ème Ch., 28 mai 2008 (contre), TGI Saint-Brieuc, 6 septembre 2007, *Min. public et a. c./ P.* (pour), in *CCE*, décembre 2007, comm. 144, pp. 32-35, note C. CARON ;
CJCE, Grande Chambre, 29 janvier 2008, *Productores de Música de España (Promusicae) / Telefónica de España SAU* (pour), www.legalis.net

de propriété intellectuelle[24], notamment dans la lutte contre le téléchargement. Nous retiendrons les analyses développées pour dégager la nature du lien entre l'identité réelle et l'identité virtuelle, d'un point de vue tour à tour objectif puis subjectif, avant de réconcilier les deux.

b) L'adresse IP, point de contact entre l'identité réelle et l'identité numérique

Le lien entre les deux identités est objectif si on considère que l'adresse IP identifie un ordinateur dont le propriétaire est lui-même identifiable. Elle peut effectivement être rapprochée d'un nom et d'un domicile. L'identité numérique cesserait donc d'être anonyme, pour devenir potentiellement nominative. C'est là une conception très concrète de l'identité virtuelle, qui s'attache avant tout à la source réelle des communications.

Mais l'ordinateur peut être utilisé par plusieurs personnes différentes. L'adresse IP a un caractère dynamique et subjectif ; son existence dans le cyberespace dépend de la volonté d'une personne, et de l'usage qui en est fait. Elle peut donc refléter autant d'identités différentes que d'utilisateurs, sans distinguer entre eux. Il suffit d'avoir à l'esprit l'exemple des cybercafés pour comprendre la relativité du lien entre les deux identités : les mêmes ordinateurs sont utilisés par une multitude d'internautes. Dans ce sens abstrait, c'est bien la volonté, subjective, qui est projetée par l'identité numérique ; cette volonté n'est pas nécessairement celle du propriétaire de l'ordinateur. L'adresse IP, qui reste inchangée, ne permet donc pas d'établir un lien certain avec une identité réelle[25].

Il est toutefois possible de réunir ces deux points de vue, en faisant preuve de pragmatisme. Si l'identité numérique reste frappée d'une grande subjectivité, l'adresse IP la rattache quand même à la réalité, ne serait-ce que parce qu'elle permet de remonter à l'ordinateur source de la connexion. La réconciliation avec l'identité réelle se fera tout simplement dans le monde réel. À supposer que le propriétaire soit celui qui s'est connecté, aucune difficulté n'est à relever. Sinon il lui appartiendra de prouver que la connexion de l'adresse IP à un moment donné est le fait d'une autre personne. Le propriétaire est alors responsable des connexions effectuées à partir de son ordinateur. Il lui appartient au moins de connaître l'identité des utilisateurs, et la période pendant laquelle ils se sont connectés. Cette obligation découle notamment de l'article 6 de la loi pour la Confiance en

---

[24] SZUSKIN L. et DE GUILLENCHMIDT M., "La qualification de l'adresse IP au centre de la lutte contre le téléchargement illicite sur les réseaux "*peer-to-peer*"", *RLDI*, n° 33, décembre 2007, pp. 6-7 ; COSTES L. et AUROUX J.-B., "L'adresse IP est bien une donnée à caractère personnel", *RLDI*, n° 31, octobre 2007, pp. 26-28.

[25] LECOMTE F. et LEMAITRE M.-H., "Inconnue juridique à cette adresse (IP) - Ou les affres du débat autour de la qualification de donnée à caractère personnel de l'adresse IP", *Expertises*, mai 2008, pp. 175-176 ; FLAMENT L., "Le numéro d'IP n'est pas une donnée à caractère personnel – La Cour d'appel de Paris persiste et signe !", note sous CA Paris, 3ème Ch., 28 mai 2008, *Droit Pénal*, décembre 2008, pp. 24-26.

l'Économie Numérique, du 21 juin 2004[26], en ce qui concerne les opérateurs de communication électroniques. La loi du 23 janvier 2006, relative à la lutte contre le terrorisme, a étendu cette obligation à toutes "*les personnes qui, au titre d'une activité professionnelle principale ou accessoire, offrent au public une connexion permettant une communication en ligne par l'intermédiaire d'un accès au réseau*" (codifié dans l'article L 34-1 du Code des Postes et des Communications Électroniques, CPCE).

Pour les cybercafés, exemple emblématique, le responsable devra relever les noms, adresses et coordonnées des clients, le poste (l'adresse IP) qu'ils ont utilisé, le début et la fin de la connexion. Ce dispositif est appliqué *de facto* dans les médiathèques publiques, afin d'identifier les utilisateurs des postes mis à disposition des usagers. Récemment encore, un jugement rendu par le Tribunal Administratif de Pau a confirmé l'exclusion d'une médiathèque d'un usager amateur de pornographie ; ce dernier a pu être identifié grâce au rapprochement des données de connexion et des horaires de réservation (nominatifs) du poste utilisé[27]. Le respect de cette exigence peut être plus délicat dans un domicile privé, où l'ordinateur familial peut être consulté par tout le monde. Là encore, il appartient à son propriétaire de créer autant de comptes qu'il y a de personnes au foyer, en plus d'assurer une obligation de surveillance, notamment à l'égard des enfants. Enfin, ce dispositif se heurte encore au développement de nouveaux logiciels d'anonymisation, qui tendent à masquer l'adresse IP[28]. Même si leur technique est encore perfectible, se pose la question de la légalité de tels logiciels au regard des développements précédents.

L'identité numérique est donc bien la projection d'une identité réelle, qui est au moins identifiable.

c) L'adresse IP, domicile virtuel ?

Sans être une donnée personnelle dans l'absolu[29], nous avons vu que l'adresse IP assure le lien juridique entre les deux identités, tant du point de vue objectif que du point de vue subjectif. Pour cette raison, elle ressort davantage du domaine de l'identifiant que de l'identité, du fait de son caractère subi[30].

Peut-être est-il possible de la rapprocher du domicile, eu égard à sa fonction de localisation physique et numérique. L'argument pourrait être examiné à l'aune de la responsabilité du propriétaire de l'ordinateur. Le

---

[26] "Les personnes dont l'activité est d'offrir un accès à des services de communication au public en ligne […] conservent les données de nature à permettre l'identification de quiconque a contribué à la création du contenu ou de l'un des contenus des services dont elles sont prestataires.".

[27] GRÉGOIRE S., "Exclusion d'un usager sur la base des données de connexion recueillies dans un espace multimédia d'une médiathèque", note sur TA Pau, 2ème ch., 18 septembre 2007, *RLDI*, n° 38, mai 2008, pp. 47-49.

[28] ITÉANU O., *L'identité numérique en question*, Eyrolles, Paris, 2008, p. 29-32.

[29] MATTATIA F., "Internet face à la loi Informatique et libertés : l'adresse IP est-elle une donnée à caractère personnel ?", *Gaz. Pal.*, 15 janvier 2008, p. 10.

[30] ITÉANU O., *op. cit.*, p. 16.

principe d'inviolabilité du domicile militerait en faveur de la qualification de donnée à caractère personnel. Si celle-ci est retenue, la collecte des adresses IP nécessite une formalité préalable auprès de la Commission Nationale de l'Informatique et des Libertés (CNIL), selon la loi Informatique et Libertés ; une telle garantie peut être rapprochée de l'article 66 de la Constitution, offrant la garantie de l'autorité judiciaire en matière de perquisition au domicile réel. Cet argument est d'autant plus d'actualité alors que la prochaine loi LOPSI 2 prévoit la faculté d'effectuer des perquisitions numériques, sur les disques durs des ordinateurs connectés, donc via l'adresse IP[31].

La qualification de "domicile virtuel", exclue pour les sites Internet du fait de leur caractère public[32], s'y prêterait donc bien, du fait de sa nature intrinsèquement personnelle, voire même privée. Celle-ci ressort clairement des données de connexion, qui identifient les "mouvements" de l'individu dans le cyberespace, leurs points de départ et/ou d'arrivée étant l'adresse IP.

B. Les données de connexion, premiers pas vers la virtualisation

Une fois l'identification assurée, la présence de l'internaute laisse un certain nombre de traces, appelées données de connexion. Ayant une fonction d'identification, elles sont un élément de l'identité numérique de l'utilisateur (1). S'il est libre de se déplacer dans le cyberespace, il reste grevé d'un bracelet électronique virtuel[33]. Ce dernier permet de rassembler les données du porteur, afin d'en tracer une identité "virtualisée" (2).

1. La constitution de l'identité numérique

Les données de connexion restituent le parcours d'un utilisateur au sein du cyberespace (a). Les textes qui leur sont applicables révèlent leur fonction d'identification, concourant à les rattacher à l'identité numérique et à leur garantir une certaine protection (b).

a) Les données de connexion, traces de pas dans le cyberespace

L'intérêt de ces données est de retracer le parcours d'un internaute. Elles permettent de savoir avec une grande précision quels sont les sites et pages qu'il a visités, incluant la durée de la connexion ainsi que ses heures de début et de fin. Toutes ces indications se font sur la base de l'adresse IP. Si celle-ci constitue la domiciliation de l'internaute au sein du cyberespace, ces données représentent les actes et les "déplacements" qu'il y effectue. Elles sont reçues et conservées par l'ordinateur connecté (historique de navigation,

---

[31] Intervention de M. ALLIOT-MARIE au Forum International de la Cybercriminalité, 20 mars 2008, disponible sur le site du Ministère de l'Intérieur, http://www.interieur.gouv.fr

[32] TGI Paris, ord. ref., 14 août 1996, *D.*, 1996, Jurisprudence, pp. 490-495, note P.-Y. GAUTIER.

[33] MALLET-POUJOL N., "Les libertés de l'individu face aux nouvelles technologies de l'information", *Cahiers Français*, n° 296, mai-juin 2000, p. 63.

cookies et données du dossier *Temporary Internet Files*), mais également par les hébergeurs des sites visités. Un certain nombre de prestataires de services sont chargés de conserver ces données, tels ceux que nous avons évoqués précédemment (opérateurs de communications électroniques, fournisseurs d'accès, hébergeurs, toute personne offrant un accès à Internet au public…). On voit déjà le rapprochement qui peut être fait avec l'adresse IP correspondante, et par là-même la personne réelle.

L'utilisation de ces données est consubstantielle à celle de l'Internet[34] pour des raisons techniques. Deux fonctions peuvent être distinguées : d'une part, elles assurent l'échange d'informations entre l'adresse IP de l'ordinateur et celle du site visité ; d'autre part, lorsqu'elles sont enregistrées, elles facilitent la connexion, en accélérant cet échange. Ainsi en est-il pour les cookies, exemple emblématique. Ces fichiers, qui s'installent réciproquement sur le disque dur de l'ordinateur et dans le serveur du site visité, évitent de répéter les informations nécessaires à la connexion et permettent de faire des statistiques sur l'usage d'un site, le tout servant à améliorer la navigation[35]. Nous verrons ultérieurement l'autre finalité qui peut leur être assignée.

Enfin, comme pour l'adresse IP, toutes ces données ont un caractère technique et dynamique. Elles concrétisent une connexion déterminée, unique, un acte de la personne dans le cyberespace. En cela, elles ne mobilisent que des éléments fragmentaires de son identité. Seul ce qui est nécessaire à l'échange informatique est actionné. L'avantage pour la personne humaine est justement de ne pas avoir à se déplacer, mais de se "décomposer" en autant informations qu'il y a d'échanges[36]. Le rassemblement de toutes ces données constitue la projection de la personne dans le cyberespace, ou du moins de sa volonté. Dans son sens numérique, il s'agit bien d'une dimension de l'identité virtuelle. Les informations en cause établissent le comportement d'un internaute sur le réseau.

Le Droit peut à nouveau aider à les rapprocher de l'identité réelle.

b) Les données de connexion, reflet des actes d'un utilisateur

Le lien avec l'identité réelle est devenu nécessaire afin d'identifier les auteurs de contenus illicites sur Internet, toujours dans le cadre de la lutte contre la cybercriminalité, le terrorisme, mais aussi le téléchargement. Outre les auteurs d'infractions, les utilisateurs des services sont également concernés, soit tout un chacun, par exemple dans la lutte contre la pédophilie. En France, l'article L 34-1 du Code des Postes et Communications Électroniques (CPCE), modifié par divers textes[37], prévoit une obligation de conservation des données, à la charge de toute personne offrant au public un

[34] FRAYSSINET J., "La traçabilité des personnes sur l'Internet", *op. cit.*, p. 76.
[35] LEROUGE L., "L'utilisation licite des cookies en droit commercial" (1ère partie), *Gaz. Pal.*, 25 janvier 2005, p. 25.
[36] DUBUISSON E., *op. cit.*, pp. 17-18.
[37] FÉRAL-SCHUHL C., *Cyberdroit – Le droit à l'épreuve de l'Internet*, 4ème éd., Dalloz, Paris, 2006, p. 104 et s.

accès à Internet ; nous renvoyons aux précédents développements concernant l'adresse IP. Cette obligation s'applique également pour les hébergeurs.

Le décret du 24 mars 2006, pris en application de la loi du 23 janvier 2006 sur la lutte contre le terrorisme, détermine quelles sont les données visées par cette obligation. Outre l'adresse IP, il s'agit principalement des données relatives : à l'identification d'un utilisateur (*login*…), aux équipements terminaux utilisés, aux caractéristiques techniques de la communication (routage, durée, volume, heure de début/de fin, protocole de référence), aux services complémentaires demandés et utilisés, aux destinataires de la communication. À cela s'ajoutent les informations administratives permettant d'identifier la personne réelle, et dont le fournisseur d'accès est détenteur. La durée de conservation des données techniques est fixée à un an par ce même décret. Notons également que l'article L 34-1 CPCE prévoit un principe d'effacement des données, dont la conservation ne constitue qu'une exception. Dans la mesure du possible, l'identification doit se limiter à un simple procédé technique[38]. L'effacement est censé assurer un caractère anonyme aux données en cause.

Ce constat nous permet d'affirmer la neutralité technique des données de connexion. Limitées au seul point de vue de l'utilisateur, elles ne représentent que son double virtuel, composé d'informations correspondant à ses connexions. Il s'agit d'un ensemble numérique distinct et anonyme. L'anonymat tombe lorsqu'on rapproche ces données de l'adresse IP, qui en est la base, et par conséquent de l'utilisateur. Dans ce cas, le lien avec l'identité réelle devient objectif ; l'identité numérique en est la projection exacte. Un grand nombre de "cyberdélinquants" a pu être identifié et localisé grâce à ce procédé, qu'il s'agisse de contrefacteurs, de terroristes, de pirates informatiques, ou encore de membres de réseaux pédophiles, pour ne citer que les exemples les plus courants.

Ce dispositif fait encore l'actualité avec le projet de loi sur la Haute Autorité pour la Diffusion des Œuvres et la Protection des droits sur Internet. Ainsi, la "riposte graduée" se fonde sur la collecte des données qui constituent l'identité numérique. Si la collecte et le traitement de telles données ont été autorisés pour les sociétés de perception et de répartition des droits d'auteur (art. 9 loi du 6 août 2004), l'identification finale ne peut être effectuée que dans le cadre d'une procédure judiciaire. Le Conseil Constitutionnel a bien sûr validé cette garantie légale[39], réaffirmé par le Conseil d'État[40], ce qui rappelle le précédent débat relatif à la qualification de l'adresse IP. La protection des droits de propriété intellectuelle doit se faire dans le respect des droits de la personnalité[41], au sein desquels nous pouvons ranger l'*habeas data* évoqué précédemment.

---

[38] BOYER J., "L'internet et la protection des données personnelles et de la vie privée", *Cahiers Français*, n° 295, mars-avril 2000, pp. 74-79.

[39] Conseil Constitutionnel, Décision 2004-499 DC, 29 juillet 2004, Loi relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, considérant n° 13.

[40] FRAYSSINET J., "Le Conseil d'État relance la CNIL dans la lutte contre la contrefaçon", *LP*, n° 243, juillet/août 2007, p. 142 (sur l'arrêt du 23 mai 2007).

[41] DERIEUX E., "Internet et protection des données personnelles", *RLDI*, n° 38, mai 2008, p. 81.

Si l'anonymat, grand avantage de l'Internet, reste de principe, sa mise en œuvre pratique paraît quand même illusoire. Relevons néanmoins que la conservation (base de l'identification) est strictement encadrée quant à sa finalité, sa durée et son utilisation[42].

Au terme de ces développements, il apparaît clairement que les données de connexion constituent un élément de l'identité numérique, tant dans leur aspect technique que dans leur aspect juridique. L'un comme l'autre se complètent. Ainsi le rapprochement de l'identité réelle est-il nécessaire pour identifier l'auteur d'un contenu ou le client d'un service. Cette faculté d'identification, rendue possible par la technique, est exigée par le Droit positif. Ce dernier établit une définition de l'identité numérique à travers ses composants, en dépit de leur caractère extrêmement dynamique. La finalité même des textes qui l'encadrent révèle le dynamisme du Droit en la matière. L'identité numérique n'existe de façon statique ni techniquement ni juridiquement. Son encadrement se justifie par le lien étroit qui existe avec la personne réelle, potentiellement victime ou coupable dans le monde virtuel.

Mais si cette première forme qu'est l'identité numérique reste neutre vis-à-vis de la personne, elle peut aussi être la base d'une identité virtualisée contre le gré de celle-ci. Nous entrons alors dans la seconde dimension de l'identité virtuelle, qui consiste à virtualiser l'identité réelle dans le cyberespace.

2. le passage forcé de l'identité numérique à l'identité virtualisée

Il est tentant de dire que ces données de connexion permettent de connaître les habitudes, goûts et centres d'intérêt de l'utilisateur dans la vie réelle. Il est légitime de penser que les sites qu'il visite reflètent des éléments de son identité personnelle ; celle-ci, à l'état d'objet, est pourtant altérée par la technique (a). Cette réification porte atteinte à l'intégrité de son titulaire, lequel doit être protégé (b).

a) l'altération technique de l'identité réelle

Le postulat de départ précité a conduit à développer des techniques de profilage des internautes, afin de personnaliser dynamiquement les services utilisés[43]. Cet aspect s'est d'abord fait sentir au niveau du commerce électronique, qui tend à cibler au maximum l'offre et la publicité en fonction des données laissées par l'acheteur[44]. Les techniques utilisées sont nombreuses et ont des finalités diverses, basées sur la construction

---

[42] MATHIAS G. et LORRAIN A.-C., "Données de connexion : un état des lieux ou une première tentative de démêlage de la toile législative", *RLDI*, n° 11, décembre 2005, pp. 54-56.
[43] DROUARD E., "Directive "Communications Électroniques" : la prospection et la traçabilité en question", *Expertises*, n° 263, octobre 2002, p. 339.
[44] MULLER A., *La net économie*, PUF, coll. Que sais-je ?, Paris, 2001, p. 101.

d'individus statistiques[45]. On distingue principalement le *profiling*, le *matching*, le *scoring* et le *data mining*. Ce dernier offre une très grande précision dans l'élaboration du profil virtuel, et permet de cerner individuellement les consommateurs potentiels. Les autres procédés ont initialement des champs d'action plus limités, comme le *scoring*, fréquent en matière bancaire[46]. Leur finalité est de dresser le profil d'une personne avec le maximum de précision. En matière informatique, ces procédés utilisent largement les données de connexion, qui permettent de connaître les sites et pages visités par l'utilisateur. Les *cookies* y sont particulièrement propices, tant leurs potentialités sont nombreuses. S'il ne s'agit ni plus ni moins que de "témoins de connexion", leur contenu inclut des informations tant sur l'utilisateur concerné que sur le site utilisé. Certains sont délibérément conçus pour collecter et transmettre des données en vue de personnaliser les services[47]. Cela leur vaut souvent le surnom de "mouchards".

Le contenu des sites et pages visités reflèteraient ainsi un intérêt potentiel de la personne connectée. Une fois le profil établi, ces mêmes services sont adaptés en fonction des informations connues de l'utilisateur. Certaines pages ou certains messages "personnalisés" apparaîtront, sur la base de ces données. Les publicités seront plus ciblées, incluant l'envoi de courriers électroniques. Les informations pourront aussi intéresser d'autres prestataires de services. Le double virtuel, fondé sur le rassemblement et la péréquation des données, représente une importante valeur marchande, s'insérant dans des méthodes de marketing qui se font de plus en plus insidieuses.

Pourtant, un certain décalage apparaît entre ce double et la personne qu'il est censé représenter. En effet, la technique, si précise soit-elle, ne peut connaître l'intention qui était poursuivie par la personne dans un acte déterminé. Les sites visités ne sont pas forcément représentatifs des centres d'intérêts de l'internaute ; la diversité des contenus librement accessibles lui permet d'aller bien au-delà. De ce fait, les données de connexion sont si fragmentaires et nombreuses que leur rapprochement permet au mieux de donner une "estimation" de la personne réelle, aussi approximative qu'un portrait-robot[48]. En aucun cas, elles ne peuvent la recomposer avec certitude. Enfin, elles n'intègrent pas le caractère aléatoire de l'adresse IP, qui n'identifie qu'un ordinateur et non une personne. Les procédés informatiques d'aide à la décision ont révélé les insuffisances de ces techniques, notamment en matière de législation sociale[49]. En effet, elles ne prennent pas en compte le facteur humain ; or celui-ci est déterminant dans tout rapport juridique,

---

[45] BOURCIER D., "Données sensibles et risque informatique – de l'intimité menacée à l'identité virtuelle", *in Questions sensibles* (KOUBI G., CHEVALLIER J., BOURCIER D. et *al.*), PUF, Paris, 1998, p. 44.

[46] GAUDEMET M. et PERRAY R., "Scoring et protection des données personnelles : un nouveau régime à l'efficacité incertaine", *PA*, 30 mai 2006, pp. 8-10.

[47] BARBRY E. et LEBON H., "Les cookies, les logiciels espions et la prospection commerciale par courriers électroniques prochainement réglementés", *Gaz. Pal.*, 24 avril 2003, p. 894.

[48] FRAYSSINET J., "La traçabilité des personnes sur l'Internet", *op. cit.*, p. 76.

[49] BOURCIER D., "Les lois sont-elles des logiciels ? L'aide à la décision en matière de législation sociale", *RFAS*, mars 1995, pp. 201-224.

incluant une certaine marge d'opportunité, d'aléatoire. Une machine ne peut intégrer toute la diversité des comportements humains. Cela nous ramène à une autre caractéristique de l'identité virtuelle, prise dans son acception numérique : la fragmentation de l'individu en informations techniques.

Ceci s'oppose à l'unicité et la permanence du corps dans le monde réel[50]. C'est bien ce qui explique l'incapacité de la technique à "résumer" les caractéristiques d'un individu. De fait, on ne peut qu'affirmer que ces procédés portent atteinte à la personne, ce qui suppose de protéger celle-ci efficacement.

b) L'atteinte réelle à l'identité personnelle

Si l'identité numérique est la projection objective de la personne, son utilisation économique porte atteinte à son intégrité. Elle trahit son identité personnelle, et en fait un objet marchand. Par transposition au monde réel, ce serait faire commerce de personnes physiques à des fins publicitaires. Les données personnelles ont quasiment acquis la nature de biens immatériels. L'identité numérique, en réduisant l'individu à une série d'informations, bouleverse la distinction entre les personnes et les biens. Il importe pourtant de maintenir celle-ci, y compris dans le cyberespace. Le lien entre l'identité numérique et l'identité réelle doit être renforcé.

Un certain nombre de textes ont déjà œuvré en ce sens, tant en droit communautaire qu'en droit national. C'est ainsi que la collecte et l'utilisation de telles données ne peuvent se faire que sous certaines conditions, qui sont principalement : le consentement de l'intéressé ; le respect du principe de finalité (la collecte doit être effectuée dans un but très précis, qui doit être porté à la connaissance de la personne visée) ; l'adéquation des données collectées à la finalité annoncée ; l'interdiction de toute utilisation ultérieure incompatible avec cette finalité ; la communication d'un certain nombre d'informations, concernant le responsable et les modalités de la collecte. Le cadre communautaire est essentiellement constitué de deux textes : la directive du 24 octobre 1995, relative à *la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données* ; la directive du 12 juillet 2002, dite "*vie privée et communications électroniques*".

En France, la loi Informatique et Libertés du 6 janvier 1978, modifiée par la loi du 6 août 2004, reprend ces mêmes exigences. La CNIL a la responsabilité de les faire respecter. À ce titre, tout traitement de données à caractère personnel doit faire l'objet de formalités préalables auprès de la commission, qu'il s'agisse d'autorisation ou de déclaration. La loi consacre par ailleurs un droit d'opposition (art. 38), un droit d'accès (art. 39) et un droit de rectification (art. 40) au profit des personnes dont les données sont collectées[51]. Les articles 226-16 et suivants du Code Pénal permettent de les protéger à juste titre. Sont ainsi réprimées les collectes qui ne respecteraient

[50] DUBUISSON E., *op. cit.*, p. 18.
[51] LUCAS A., DEVÈZE J. et FRAYSSINET J., *Droit de l'informatique et de l'internet*, PUF Droit, Thémis Droit privé, Paris, 2001, pp. 99-121.

pas les exigences posées par la loi (art. 226-17) ou qui seraient effectuées par des moyens frauduleux ou illicites (art. 226-18). Il en est de même lorsqu'elles portent atteinte aux droits des personnes. Ainsi en est-il lorsque l'utilisation des données se fait pour une autre finalité que celle de leur collecte (art. 226-21), lorsqu'elles sont transmises à des tiers qui n'ont pas qualité pour les recevoir ou portent atteinte à la considération et l'intimité de la vie privée de la personne concernée (art. 226-22). Ces délits sont passibles de peines pouvant aller jusqu'à cinq ans d'emprisonnement et 300 000 euros d'amende. Nous ne citons là que les plus essentiels.

L'ensemble de ces dispositions pénales, de ces droits, obligations et exigences, doit permettre de protéger efficacement les personnes contre l'utilisation abusive de leurs données de connexion. En ce qui nous concerne, nous dirons qu'elles rapprochent l'identité numérique et l'identité réelle des internautes. Ainsi ces derniers peuvent, en principe, conserver le contrôle de leurs données. L'intégrité de l'individu est juridiquement protégée au sein du cyberespace, comme elle l'est dans le monde réel. Sur le plan civil, l'existence implicite d'un droit à la protection des données personnelles, ou droit au respect de l'identité, peut être démontrée avec un fondement distinct de l'article 9 du Code Civil[52]. Ce dernier est impropre eu égard à la nature des informations en cause. Les nouvelles technologies dépassent les simples limites de la vie privée et atteignent directement l'intégrité de la personne, notamment dans son identité. L'*habeas data*, évoqué précédemment, resurgit à ce niveau.

L'identité réelle et l'identité numérique se doivent d'être le plus possible en adéquation. C'est pourquoi l'identité virtualisée, prise dans ce premier sens comme un lien entre les deux, doit être contrôlée par son titulaire. Autrement, elle constitue une atteinte illégitime, rompant le lien qui doit exister avec la réalité aux dépens de l'individu… Ce serait toutefois oublier que ce dernier a aussi la maîtrise des éléments qu'il divulgue. À ce titre, la virtualisation peut aller bien plus loin, confinant à l'usurpation ou la "fabrication" d'identité.

II. L'identité virtuelle, copie servile de l'identité réelle

Par-delà les données numériques, l'identité virtuelle peut revêtir d'autres formes dans le cyberespace. La cyberculture tend en effet à valoriser la personnalisation des pratiques. L'usage de la messagerie électronique, le recours aux noms de domaine intègrent déjà des éléments d'identification. Mais de manière générale, les internautes sont de plus en plus sollicités sur leur identité, au point que certains services leurs sont entièrement dédiés. Cependant, les moyens techniques mis en œuvre dans le cyberespace assurent une totale marge de manœuvre aux utilisateurs, qui restent maîtres de leurs éléments d'identification.

En reprenant notre distinction, nous sommes ici face à la deuxième et la troisième dimension de l'identité virtuelle, autrement dit l'identité

---

[52] MARINO L., *op. cit.*, p. 1482-1483.

virtualisée et l'identité immatérielle. La deuxième dimension se divise elle-même en deux catégories de données : d'une part, les données de connexion telles que schématisées par les logiciels de traçabilité (cf. première partie) ; d'autre part, les données de l'identité réelle, telles que divulguées dans le cyberespace. Nous nous intéresserons maintenant à cette deuxième catégorie. Elle comprend les éléments d'identification et tout ce qui caractérise la vie personnelle de l'individu.

L'étude des éléments d'identification révèle une confusion entre le nom patronymique et le pseudonyme, soulevant l'ambivalence de cet aspect de l'identité virtuelle (A). L'incertitude est accentuée lorsque les éléments de la vie personnelle sont aussi transposés au monde virtuel ; dans ce cas, l'identité réelle sera "violée" par l'identité virtuelle. Enfin, celle-ci peut tendre à s'en détacher au maximum dans la troisième dimension, l'identité immatérielle ; totalement artificielle, elle reste pourtant rattachée à la réalité (B).

A. Le nom patronymique, pseudonyme de l'identité virtualisée

Si le nom constitue le repère de l'identité de la personne[53], c'est notamment parce qu'on le reçoit de façon généalogique. Tel n'est point le cas dans le cyberespace, où l'individu a le choix de sa dénomination. Un tel confort suscite une série d'interrogations. En effet, le nom peut aussi bien être décliné par son titulaire que par une tierce personne, pour des raisons diverses. Il importera alors de le protéger contre des usages incertains (1). Face à ces menaces, l'utilisateur peut se dissimuler derrière un pseudonyme, sans que cela soit pourtant exempt de risques (2).

1. L'usage incertain du nom patronymique comme identifiant virtuel

Un grand nombre de services dans le cyberespace recourent à l'usage du nom, ou plutôt d'une "dénomination", pour des finalités diverses. Si celle-ci devrait être réelle, l'internaute n'est nullement obligé de la respecter (a). Les nombreux abus qui peuvent être commis seront sanctionnés par des procédés de droit commun, qui peuvent encore être renforcés (b). Les remarques qui suivent peuvent être étendues au prénom, bien que de nature différente.

a) L'exigence illusoire d'un nom dans le cyberespace

Les services les plus élémentaires de l'Internet se basent sur la présentation d'un nom, que l'on voudrait être réel.

Ainsi en est-il de l'adresse mail ou du nom de domaine, références exemplaires. Le recours à un nom est nécessaire afin d'identifier objectivement une personne ou un service, chose qui n'est pas possible si

---

[53] CORNU G., *Droit Civil – Introduction, les personnes, les biens*, 12ème éd., Montchrestien, Paris, 2005, p. 277.

l'on s'en tient aux seules données techniques. L'identité est indispensable pour établir une communication. Nous avons déjà vu que le nom de domaine était initialement considéré comme la traduction "littéraire" de l'adresse IP. Il en est de même pour l'adresse mail, qui permet d'établir une communication épistolaire et directe, sans être systématiquement privée. Leur fonction tend à les rapprocher de celle que remplissent le nom ou le domicile dans la vie sociale[54]. La tension vers la réalité est ici légitime ; elle permet de dépasser l'aspect technique du cyberespace, inaccessible aux sens de l'être humain. Par-delà ces nécessités pratiques, l'identification réelle est encore exigée en termes de consentement lors d'un échange informatisé ; la notion d'identité virtuelle a initialement été envisagée à ce niveau[55]. Elle est aussi demandée dans un grand nombre de services, liés principalement au commerce électronique ; ainsi, il est d'usage de remplir un formulaire d'inscription avant d'accéder à un site de vente en ligne, un forum, un blog…

Si tous ces services misent sur l'honnêteté de l'utilisateur, c'est sans compter sur l'immense potentiel qui est en son pouvoir. En effet, l'internaute, au-delà des données techniques, est parfaitement libre de divulguer ses noms et prénoms réels comme de s'en fabriquer ou, pire encore, d'inscrire ceux d'une autre personne. La tendance est réelle, et reflète une crainte des utilisateurs à voir leur identité circuler sur les réseaux[56]. La peur est d'autant plus grande que ces données, rendues publiques, sont librement accessibles, ne serait-ce que par les moteurs de recherche, qui permettent une collecte indirecte[57], mais également par des logiciels "aspirateurs"[58].

De plus, les facilités laissées dans le choix de la dénomination permettent à un internaute mal intentionné d'usurper l'identité de quelqu'un à des fins frauduleuses. Le nom d'autrui peut être utilisé afin de dissimuler le vrai coupable d'un délit réel commis sur Internet[59]. L'usurpation peut aussi avoir des fins diffamatoires[60] ou publicitaires[61]. De nombreux contentieux sont déjà intervenus à ce niveau, soulignant les abus portés au nom patronymique, et démontrant le caractère très incertain de cet élément d'identification dans le cyberespace. Les noms de domaine et adresses électroniques sont propices aux utilisations frauduleuses les plus diverses. Mais n'importe quel service à caractère nominatif est concerné, comme par

---

[54] GAUTIER P.-Y., "L'e-mail", *in Clés pour le siècle*, Dalloz, Paris, 2000, p. 372.
[55] CAPRIOLI E., "Consentement et systèmes informatiques", *in Droit et intelligence artificielle – Une révolution de la connaissance juridique* (ss la dir. de BOURCIER D., HASSETT P. et ROQUILLY C.), Romillat, Collection Droit et technologies, Paris, 2000, pp. 120-125.
[56] Selon diverses études menées aux États-Unis, 41 % des internautes américains affirment se déconnecter d'un site qui leur demande des informations personnelles, et 40 % préfèrent communiquer de faux renseignements.
[57] FENOLL-TROUSSEAU M.-P., "Les moteurs de recherche : un piège pour les données à caractère personnel", *CCE*, janvier 2006, p. 22.
[58] LEPAGE A., "Collecte déloyale de données personnelles sur Internet", note sous Cass. Crim., 14 mars 2006, *CCE*, septembre 2006, pp. 43-44.
[59] MANARA C., "Conditions de la sanction de l'usurpation de nom sur Internet", note sous Cass. Crim., 29 mars 2006, *D.*, 2006, Actualité Jurisprudentielle, pp. 1443-1444.
[60] TGI Paris, ord. ref., 28 juin et 31 juillet 2000 (concernant notamment l'utilisation abusive du nom de Bertrand Delanoë) , *CCE*, novembre 2000, pp. 24-25, note A. LEPAGE.
[61] TGI Nanterre, 13 mars 2000, *D.*, 2000, Jurisprudence, pp. 275 276, note A. LEPAGE.

exemple les blogs, chats, réseaux sociaux… suscitant autant de craintes légitimes qui renforcent le désir d'anonymat et de dissimulation des utilisateurs.

b) La trahison du nom sanctionnée par le droit commun

Le droit commun assure la protection du nom des personnes, que l'usurpation soit volontaire ou non. Dès lors qu'elle est dommageable, la responsabilité civile peut aisément être actionnée, de même que la responsabilité pénale, pour certains délits.

Même si l'usurpation est involontaire, il existe différents moyens de régler l'utilisation qui en est faite. Un important contentieux a déjà réglé les rapports entretenus entre le nom patronymique et les propriétés incorporelles[62]. La transposition de ses principes aux conflits de noms de domaine peut très bien être poursuivie pour le nom des personnes[63]. Ainsi, dès lors qu'un risque de confusion est avéré entre le titulaire du nom et son utilisateur, le premier doit pouvoir faire cesser l'appropriation indue par le deuxième, sauf exception particulière du pseudonyme (voir *infra*).

Par ailleurs, il serait envisageable de développer dans le monde virtuel l'action en "contestation de nom". Bâtie par la jurisprudence sous des dénominations diverses, cette action n'est actuellement visée par aucun texte en droit français, même pas par le Code Civil. Son but est de faire cesser l'utilisation du nom par un tiers, quels qu'en soient la forme et le but[64]. Cette action autonome ne suppose pas l'intention de nuire, bien qu'elle soit souvent confondue avec l'action pénale. Le simple fait qu'une personne utilise un nom qui n'est pas le sien constitue une violation de la règle de l'indisponibilité du nom, consacrée par la loi du 6 fructidor An II. Une confusion suffit pour exercer l'action.

Elle est toutefois limitée par les cas où l'utilisateur s'est approprié licitement l'usage du nom. Il n'y a guère qu'en termes d'usage commercial, spécialement pour les noms de domaine, qu'une telle appropriation pourrait avoir lieu, sous la réserve d'une éventuelle confusion. L'hypothèse d'une appropriation par prescription est tout à fait impossible dans le cyberespace, la possession prolongée d'un nom patronymique ne pouvant y être reconnue. Quand bien même ses conditions de durée, de publicité et de loyauté[65] seraient vérifiées, il faut avoir à l'esprit que les "personnes virtuelles" présentes dans ce cyberespace n'ont pas d'intelligence autonome, restant sous le contrôle d'individus bien réels, dont le nom sera différent. Elles ne peuvent donc revendiquer l'usage virtuel d'un nom que sous certaines conditions, que nous verrons dans le cadre du pseudonyme.

---

[62] COLOMBET C., "Le nom et les propriétés incorporelles", *D.*, 1989, Chronique, pp. 31-38.
[63] FAUCHOUX V. et BEAURAIN N., "Règlements des conflits de noms de domaine : vers l'élaboration d'un droit *sui generis* ?", *LP*, n° 169, mars 2000, pp. 15-20.
[64] NÉRAC P., *La protection du nom patronymique en droit civil*, Thèse Lille, 1975, p. 27.
[65] CHAMOULAUD-TRAPIERS A., "La possession du nom patronymique", *D.*, 1998, Chronique, pp. 39-46.

De plus, face à l'immensité du cyberespace, face au nombre incommensurable d'informations qui y circulent, la possibilité d'effectuer d'une action en contestation paraît bien illusoire. Les cas de rencontres fortuites risquent de plus d'être fréquents. Enfin, cela oblige à opérer une distinction entre services de même nature, selon qu'ils aient un caractère nominatif ou non ; l'adresse mail est particulièrement concernée[66]. Si la reconnaissance d'une action en contestation de nom autonome militerait en faveur du droit au respect de l'identité, sa mise en œuvre pratique se heurterait à beaucoup de difficultés.

Sur le plan pénal, l'usurpation n'est à ce jour sanctionnée que lorsqu'elle implique une intention délictueuse. L'article 434-23 du Code Pénal réprime, en tant qu'entrave à l'exercice de la Justice, "*le fait de prendre le nom d'un tiers, dans des circonstances qui ont déterminé ou auraient pu déterminer contre celui-ci des poursuites pénales*". L'efficacité de ce texte ne doit pas être mise en doute, dès lors que la constatation du préjudice pour le tiers usurpé est rendue publique sur les réseaux. De plus, la dissimulation ne peut tenir en tant que telle, l'identité numérique permettant de remonter jusqu'au coupable (voir *supra*). Enfin, reste le cas des nouvelles formes d'usurpation, celles qui, tout en étant volontaires, ne rentre pas dans le cadre du délit précité. Nous y reviendrons par la suite, ce phénomène dépassant le cadre de la dénomination.

L'identité virtuelle est insaisissable. L'incertain domine, le doute persiste sur l'usage du nom. Une solution simple serait d'obliger les internautes à s'identifier sous leur exacte dénomination, et de sanctionner toute utilisation indue du nom d'autrui. Il faudrait alors vaincre le désir d'anonymat de la majorité des internautes. Cette solution aurait l'avantage de mettre l'identité virtualisée en adéquation avec l'identité réelle ; par ailleurs, l'internaute conserverait une totale liberté dans sa virtualisation.

Face aux craintes, la plupart des utilisateurs préfèrent utiliser un pseudonyme. Ce repli, s'il est compréhensible, n'offre pas toute garantie non plus.

2. L'incertitude du pseudonyme comme élément de l'identité virtualisée

Le cœur de la virtualisation de l'identité se situe au niveau du pseudonyme. C'est de la liberté laissée dans le choix de la dénomination que peut naître le décalage entre l'identité réelle et l'identité virtuelle (a). Face aux risques qui viennent d'être évoqués, ce décalage permet de préserver un certain anonymat, et de se protéger contre l'utilisation des données personnelles. En poussant la virtualisation à son comble, il serait possible de distinguer totalement les deux identités, ce qui offre l'avantage de la simplicité, sans exclure tous les risques (b).

---

[66] MANARA C., "Aspects juridiques de l'e-mail", *Dalloz Affaires*, n° 149, 19 février 1999, p. 280.

a) La banalisation discutable du pseudonyme dans le cyberespace

Le cyberespace bouleverse la nature du pseudonyme. Toute personne peut accéder au confort du choix de sa dénomination, privilège réservé jusqu'à présent aux personnalités du monde littéraire et artistique. Défini par la jurisprudence comme "un nom de fantaisie choisi par une personne pour masquer au public sa véritable personnalité en fonction d'une activité particulière", il constitue une propriété incorporelle et confère un droit privatif à son titulaire, par la notoriété qu'il acquiert[67]. La définition précitée est parfaitement transposable au monde virtuel, et applicable à toute personne. Le caractère public de l'usage, condition primordiale pour sa reconnaissance, ne fait aucun doute. Celui-ci subsiste pour l'exigence d'une activité particulière, entendue le plus souvent comme une activité littéraire et artistique ; quelque part, celle-ci est désormais accessible au plus grand nombre dans le cyberespace, qu'il s'agisse d'écriture, de musique, d'audiovisuel… Les services du web 2.0 y sont particulièrement propices. Ainsi, la plupart des utilisateurs se présentent sous un pseudonyme pour écrire sur un forum, un blog, pour poster des photos, des vidéos… L'existence d'un public indéterminé et non quantifiable justifie l'usage du pseudonyme de ce point de vue. Le simple exercice d'une activité dans le monde virtuel peut paraître particulier. Au-delà, il reste tous les risques auxquels s'exposent les données personnelles, et qui justifient la dissimulation.

Le risque principal qui apparaît est le recours au nom d'une autre personne. Celui-ci peut être volontaire, lorsque le nom est notoire, ou involontaire. Nous avons déjà vu comment un tel usage peut être contesté par le titulaire du nom. Reste le cas où la personne a acquis l'usage de ce pseudonyme de façon légitime, et sans risque de confusion. Dans ce cas-là, la distinction avec le nom patronymique sera totale. Celle-ci sera déterminée par la réunion des conditions propres à l'usage du pseudonyme dans le monde réel, à savoir la durée, la notoriété et la spécialité de l'activité.

La transposition de ce faisceau d'indices aux dimensions exceptionnelles du cyberespace laisse quand même planer le doute. Elle n'est pourtant pas inconcevable, certaines personnes ayant acquis une notoriété publique dans le cyberespace sous un pseudonyme particulier. Mêmes les services les plus anodins, tels que les blogs ou forums, ont leurs "membres d'or", connus sous un nom qui n'est peut-être pas le leur. Faudrait-il alors reconnaître l'acquisition du nom patronymique au titre d'un pseudonyme ? La problématique que nous avons esquissée précédemment prend toute sa signification. En effet, le cyberespace facilite une telle acquisition, d'une part par son caractère public, d'autre part parce que les risques de confusion sont plus improbables dans l'immensité de la toile. La rencontre fortuite y est plus probable.

---

[67] LINDON R., *Une création prétorienne : les droits de la personnalité*, Dalloz, Paris, 1974, pp. 136-137.

Les risques ne sont cependant pas exclus, du fait que l'internaute reste libre de dévoiler sa véritable identité ou de la masquer.

b) La distinction relative des deux identités dans le cyberespace

Pour simplifier les choses, il faudrait admettre que le nom utilisé dans le monde virtuel n'est qu'un pseudonyme. Il serait juridiquement distinct de l'identité réelle, en dépit des coïncidences.

Cette tension est inverse de celle que nous avons évoquée dans la précédente partie, qui exigerait que la dénomination utilisée soit celle de l'identité réelle afin de prévenir tout risque de confusion. Or le droit de se voiler n'est pas réservé aux artistes, mais appartient à tout un chacun. Cette deuxième solution permettrait de distinguer plus nettement identité réelle et identité virtuelle, tout en assurant une certaine sécurité juridique. À l'inverse de la première, elle ne nécessite pas de mise en œuvre particulière et respecte la liberté individuelle des internautes. Chacun conserverait le choix de sa dénomination et pourrait en user sans porter atteinte aux droits des tiers. L'identité réelle serait préservée, et l'internaute aura son pseudonyme pour le monde virtuel. Si les deux coïncident, il peut en être fait mention par le titulaire, ce qui est déjà le cas dans bien des services[68]. Le lien est maintenu par l'identité numérique, tout en laissant le bénéfice d'un anonymat relatif à l'internaute. Mais cette solution, aussi idéaliste que la première, reste bien utopique du fait de la liberté laissée à ce dernier.

De ce fait, si le recours au pseudonyme reste de principe pour se protéger, le choix d'un nom de fantaisie, imaginaire, paraît être la solution la plus adéquate. Mais les risques persistent. En effet, il n'est jamais exclu que ce nom soit déjà utilisé et porte atteinte aux droits de tiers. Ce peut être le cas notamment en termes de nom de domaine, de marque commerciale, ou tout simplement au titre de la dénomination d'une autre personne. Dans ce dernier cas, comment faire valoir l'antériorité[69] ? Pour les autres, comment cerner les risques de confusion ? C'est que l'utilisation de l'identité réelle revêt aussi un intérêt commercial, lorsque des entreprises déclinent leurs services sur l'Internet. L'utilisation d'une raison sociale comme nom de fantaisie peut porter atteinte aux droits de la société. Enfin, quelle valeur accorder à un engagement passé sous un pseudonyme ? Le lien avec l'identité réelle doit quand même être établi, ce qui rend le pseudonyme bien illusoire. L'anonymat ne peut être total, sauf à exécuter une procédure des plus contraignantes lors de la connexion[70].

Au final, l'identité virtualisée peut respecter ou trahir l'identité réelle, ce qui la rend toujours insaisissable. Les risques de confusion sont importants et concernent tout utilisateur connecté. Les deux solutions radicales que nous avons évoquées règleraient le problème : soit distinguer totalement les deux identités, en considérant que le nom virtuel n'a qu'une valeur de

[68] Exemple : dans les réseaux sociaux, les profils officiels d'hommes politiques sont mentionnés en tant que tels, afin de les distinguer des "fakes".
[69] LINDON R., *op. cit.*, p. 181.
[70] ITÉANU O., *op. cit.*, pp. 25-32 (les sept règles de l'anonymat).

pseudonyme ; soit imposer la conformité des deux noms. La réalité se situe à mi-chemin, à savoir qu'il faut distinguer entre les données objectivement conformes à la réalité, et celles qui sont décalées. Cependant, le droit positif évolue plutôt vers la deuxième solution, comme nous le verrons par la suite.

La situation se complique lorsque, sur la base d'une dénomination, la virtualisation va jusqu'à recréer ou rejeter l'identité personnelle de l'individu.

B. De l'identité virtualisée à l'identité immatérielle : projection ou rejet de l'identité réelle

Passé le stade de l'identification et ses controverses, vient la projection complète de l'identité personnelle. Celle-ci est entendue au sens le plus large, incluant les éléments d'identification, mais aussi tous les points de repères, de fait ou de droit, qui définissent un individu, qui le font se sentir lui-même (tels que le sexe, la religion, les opinions, goûts, relations amicales, professionnelles…). Un recoupement peut être fait avec la vie privée, en ce qui concerne ses composants, sans que l'on puisse affirmer qu'il y ait une totale confusion. À ce stade, nous sommes encore dans l'identité virtualisée, dont nous achevons l'étude. Elle peut à nouveau être en adéquation ou en décalage avec l'identité réelle. De plus, ses éléments constitutifs doivent plus que jamais faire l'objet d'une protection (1).

Enfin, il existe certains services ou pratiques qui excluent d'office l'identité réelle, tendant vers l'identité immatérielle la plus absolue. Le cas de l'avatar de jeu vidéo est le plus célèbre, se distinguant totalement de la réalité… il ne cesse pourtant d'interagir avec elle (2).

1. L'identité réelle recherchée ou violée par la virtualisation

La personnalisation des pratiques est devenue caractéristique avec le développement du Web 2.0. La toile rapproche des personnes réelles ; le média qu'elle constitue se doit donc de refléter au maximum la réalité. Mais l'internaute bénéficie toujours d'une totale liberté de choix et d'invention. Si certains services sont entièrement dédiés à la projection détaillée de l'identité réelle (a), celle-ci peut toujours faire l'objet d'un certain décalage, voire même de violations graves contre lesquelles il faudra la protéger (b). Nous examinerons ces difficultés à travers l'exemple des réseaux sociaux, comme Myspace ou Facebook.

a) La mise à nue collective de l'identité réelle

L'intérêt des réseaux sociaux est de fournir à l'internaute une page personnelle, vouée à recevoir, outre ses noms, prénoms, date et lieu de naissance, des éléments relatifs à son identité personnelle : opinions politiques, orientation sexuelle, centres d'intérêts, goûts artistiques et culturels, activités professionnelles et privées, photographies (qui peuvent être nominatives), vidéos, souvenirs… le tout agrémenté de liens hypertextes vers les pages de ses amis ou de ses sites préférés. Il est également invité à créer ou intégrer des groupes, reflétant ses centres d'intérêt ou traits de

personnalités, une fois encore avec force de détails. Des albums photos peuvent être constitués, avec la liberté de laisser des commentaires. Comme si cela ne suffisait pas, l'utilisateur est régulièrement démarché par des questionnaires en tout genre, présentés sous la forme de jeux, mais destinés à lui faire dévoiler toujours plus d'éléments personnels. Les résultats sont de plus mis en partage, l'application devant être envoyée à tous les contacts d'une personne pour fonctionner correctement. Enfin, des fonctions permettent de connaître toutes les actions d'un membre du réseau, allant jusqu'à donner l'heure exacte à laquelle elles ont été effectuées.

Si l'Internet opérait initialement un éclatement de l'individu en une multitude de données numériques fragmentaires, ces réseaux tendent à reconstituer la personne, dans son intégrité, avec encore plus de détails que l'on ne pourrait en connaître lors d'une rencontre dans le monde réel. C'est exactement comme si l'individu était mis à nu, et soumis à une exposition généralisée à tous les autres internautes. N'exagérons pas pour autant. Ce n'est que la vision la plus absolue des réseaux sociaux, lesquels restent soumis au principe de la liberté de l'utilisateur. Il appartient à celui-ci de mesurer et surveiller les données qu'il divulgue s'il veut se protéger. Les risques sont à nouveau bien réels, en dépit des beaux discours assénés par les responsables de ces réseaux. Récemment, un désaccord est intervenu entre Google, Facebook et Myspace concernant la portabilité des données, sorte d'interopérabilité de tous les réseaux sociaux[71].

Du point de vue du Droit, la majorité des informations présentes sur ces réseaux constitue des données à caractère personnel, et certaines ne peuvent faire l'objet d'une collecte au sens de la loi Informatique et Libertés[72] ; même si, en principe, la collecte de telles données est possible lorsque la personne y a explicitement consenti (art. 8, II, 4° loi IFL), on ne saurait déduire un tel consentement de la divulgation volontaire des informations. De plus, dans l'hypothèse où le traitement des données pourrait porter atteinte aux droits et libertés de la personne, un deuxième consentement est exigé (art. 7., 5° loi IFL), concernant précisément la finalité poursuivie. Cette disposition s'applique particulièrement aux traitements qui ne reposent pas sur une collecte directe auprès des personnes concernées[73], ce qui inclue les cas où elles ont elles-mêmes divulgué les données en cause. La règle est ici analogue à celle de l'article 9 du Code Civil, qui protège les informations relatives à la vie privée. Même dans le cas où elles ont fait l'objet d'une divulgation antérieure par le principal intéressé, leur utilisation reste soumise à consentement. Par conséquent, c'est non seulement la

---

[71] ASTOR P., "Réseaux sociaux : Myspace data Availability veut organiser la portabilité des données de profil", *Zdnet*, 11 mai 2008, http://www.zdnet.fr
DUMOUT E., "Facebook et Google déjà en conflit sur la portabilité des données", *Zdnet*, 16 mai 2008, http://www.zdnet.fr

[72] Art. 8 al. 1 : "Il est interdit de collecter ou de traiter des données à caractère personnel qui font apparaître, directement ou indirectement, les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes, ou qui sont relatives à la santé ou à la vie sexuelle de celles-ci."

[73] FRAYSSINET J., "Note2be.com : la notation ou pas des enseignants, telle est la question…", *RLDI*, n° 38, mai 2008, pp. 30-36.

collecte mais aussi la réutilisation de ces données par une autre personne qui est prohibée. Sur le plan pénal, les articles 226-16 et suivants du Code Pénal trouveront à nouveau à s'appliquer, au même titre que pour les données de connexion.

Mais la circulation des informations est largement rendue possible dans les réseaux sociaux, et sur l'Internet en général. De ce fait, hors les cas de collecte et traitement à grande échelle, les données peuvent être récupérées, utilisées ou déformées de façon individuelle. La fabrication intellectuelle[74] de l'identité des personnes, rendue possible dans le cyberespace, est largement incontrôlable. Il importe à nouveau que la personne soit protégée contre ces utilisations, ce que le droit positif garantit déjà dans une large mesure.

Prenons l'exemple de l'image des personnes. Il est toujours possible, sur les réseaux sociaux, de télécharger les photos laissées par une personne, d'y ajouter des commentaires, de donner des précisions sur une situation compromettante, de ressortir des photos oubliées… Or l'image est une donnée d'identification, soumise à la loi IFL. Même si celui qui publie la photo s'abstient de mentionner le nom des personnes représentées, l'image de celles-ci reste une donnée d'identification. Malgré l'absence de légende, lesdites personnes peuvent voir leur image publiée dans une totale ignorance, en violation des dispositions qui protègent les données à caractère personnel mais aussi de l'article 9 du Code Civil. Rappelons que toute personne se voit dotée, sur ce fondement, d'un droit à l'image autonome et absolu. Il permet de s'opposer à la publication de son image, quelle qu'en soit la finalité. Or il faudrait que les internautes puissent "éplucher" méthodiquement les pages du réseau pour prévenir tout risque, ce qui est physiquement impossible. On peut se demander si le rattachement à la vie privée n'est pas trop réducteur, de par le caractère autonome de la protection ainsi accordée. La même caractéristique peut être relevée à l'égard du droit au nom (vue à travers l'action en contestation de nom).

Sur le plan pénal à nouveau, les données relevant de l'identité sont protégées au titre de certains délits. La diffamation et l'injure, prévus par la loi du 29 juillet 1881, trouveront un champ d'application particulièrement large, lorsque les informations seront réutilisées à de telles fins. Tel est le cas sur Facebook, notamment avec le développement des groupes de discussion, qui peuvent viser une personne précise dans une totale liberté d'expression. Si l'intention peut paraître louable de prime abord, la liberté laissée aux internautes peut conduire à des excès condamnables. Les groupes permettent de disserter de l'identité d'un individu lambda, d'en révéler les qualités, les défauts, les erreurs… le tout faisant l'objet de discussions, moqueries ou évaluations. Le culte de la performance, très en vogue dans notre société, s'y exprime particulièrement, allant jusqu'à la notation des informations, et la comparaison entre les personnes. Le récent scandale du site Note2be n'est

[74] RAVANAS J., *La protection des personnes contre la réalisation et la publication de leur image*, LGDJ, Paris, 1978, pp. 37-38.

que la partie émergée de l'iceberg[75]. Ce principe de "performance" dépasse largement les seuls réseaux sociaux. Il en est de même pour les photographies laissées en libre accès et qui peuvent donner lieu à des montages non autorisés, réprimés par le Code Pénal[76], ainsi qu'à l'usurpation d'identité, comme nous le verrons par la suite.

Toutes ces dispositions, civiles ou pénales, démontrent à nouveau l'existence implicite du droit au respect de l'identité. Un tel droit mériterait l'avantage d'être autonome, distinct de tout autre fondement, afin de protéger l'identité contre toute utilisation non autorisée. Un rapprochement peut être fait avec la notion de *false light*, reconnue par la jurisprudence et la doctrine américaines. Celle-ci implique un élément de fausseté, de déformation, dans l'utilisation des données personnelles[77]. Proche de la diffamation, elle s'en distingue par un champ d'application plus large, sanctionnant le décalage avec la réalité, l'attribution de fausses données à une personne, la trahison de son identité. Cet argument a notamment été appliqué, en matière de presse, à la réinterprétation fausse ou hors contexte de photographies. Le recours à cette notion américaine renforcerait l'autonomie du droit au respect de l'identité. Le développement du cyberespace cette conception nouvelle. La protection de la vie privée, ou de la dignité, ressurgirait quand même en fonction des éléments contextuels. L'application de ce droit est plus que jamais nécessaire dans le cyberespace, bien que techniquement difficile à assurer. La nature même des services en cause s'y oppose.

Nous le voyons bien avec les réseaux sociaux, qui révèlent l'intégrité de la personne avec le soutien de ses relations en totale violation de son identité. La masse emporte les individus et les poussent à se déshabiller les uns les autres. Ils sont de plus exposés à de grands risques de collecte, implicite ou explicite, notamment à des fins publicitaires[78] au même titre que les données de connexion. Rappelons enfin qu'il ne s'agit que d'un exemple particulier. L'ensemble des services de l'Internet permet une circulation à grande échelle d'informations du même type (photos, commentaires, faits divers…).

Mais si l'adéquation entre identité réelle et identité virtuelle est encore recherchée dans les réseaux sociaux, la virtualisation permet aussi à la seconde de violer la première.

---

[75] GUILLEMIN C., "Note2be.com jugé "illégitime" par la Cnil", *Zdnet*, 7 mars 2008, http://www/zdnet.fr

[76] Article 226-8 du Code Pénal : "Est puni d'un an d'emprisonnement et de 15000 euros d'amende le fait de publier, par quelque voie que ce soit, le montage réalisé avec les paroles ou l'image d'une personne sans son consentement, s'il n'apparaît pas à l'évidence qu'il s'agit d'un montage ou s'il n'en est pas expressément fait mention."

[77] RIGAUX F., *La protection de la vie privée et des autres biens de la personnalité*, LGDJ, Paris, 1990, pp. 311-312.

[78] McCARTHY C., "Facebook renonce à imposer son programme publicitaire Beacon", *Zdnet*, 6 décembre 2007, http://www.zdnet.fr

b) La sanction future de l'usurpation autonome

L'usurpation est plus que jamais rendue possible. Même si elle a toujours existé, l'Internet la met à la portée de tous, tout simplement parce que les individus ne sont pas en présence physique les uns des autres. Sa portée sera bien plus large que celle du simple nom patronymique. Les réseaux sociaux nous fournissent à nouveau un exemple frappant.

La constitution d'un faux profil est devenue chose fréquente, spécialement pour les personnalités publiques ou politiques. Ces derniers se sont ainsi trouvés dans l'obligation de valoriser leur profil officiel. Certes, leur fonction les expose naturellement à la critique et la caricature, dans les limites du respect de la vie privée et des autres délits de presse. Mais il est étonnant de relever que ces *fakes* n'ont nullement cet objectif. D'une grande sobriété, ils se présentent tout simplement comme le profil réel de la personne nommée. Les choses s'aggravent dès lors que l'Internet rend cette faculté d'usurpation accessible à tout utilisateur des réseaux, toute personne pouvant également en faire l'objet. N'importe qui pourra donc se faire un faux profil, avec le confort d'une identité très réaliste. Ce faux profil pourra usurper l'identité d'un tiers, (in)volontairement, à des fins très diverses qui peuvent être sérieuses. Il ne visera pas nécessairement la diffamation ou l'injure, au sens de la loi du 29 juillet 1881, ni même la dissimulation d'identité, telle qu'elle est entendue par l'article 434-23 du Code Pénal (voir *supra*). En effet, cette usurpation, bien que volontaire, n'induit pas forcément des poursuites contre la personne usurpée. De fait, nous pouvons parler d'usurpation autonome.

Si nous avons commencé par affirmer que l'Internet réduisait l'individu en une série de données numériques, cette innovation nous amène à réviser quelque peu le propos : en effet, c'est aussi en informations bien réelles et compréhensibles que la personne se trouve éclatée. Celles-ci sont réduites à l'état de choses, ignorant totalement l'intégrité de la personne. Si la maîtrise de l'image d'une personne a très tôt posée problème en matière artistique[79], et si elle s'est étendue aux autres données en matière de presse, l'Internet renouvelle cette problématique avec un champ d'application exceptionnel. Toute personne peut maintenant y récolter les informations relatives à une personne, et recomposer son profil avec un certain réalisme. Il importe pourtant de protéger la personne contre toute utilisation de ces éléments, qui dépassent l'image et le nom.

Ce type d'usurpation n'est actuellement pas visé par le droit positif. De nombreuses propositions ont cependant été faites afin de pénaliser cette nouvelle forme de violation de l'identité, notamment aux États-Unis[80] et en France. C'est ainsi qu'une proposition de loi tendant à "*la pénalisation de l'usurpation d'identité numérique sur les réseaux informatiques*" a été déposée en 2005 par le sénateur Michel Dreyfus-Schmidt, prévoyant d'insérer un nouvel article 323-8 dans le Code Pénal. La nouvelle

[79] Voir la célèbre affaire *Whistler*, Cass., Civ., 14 mars 1900, *D.*, 1900, I, 497.
[80] Essentiellement avec le Identity Theft and Assumption Deterrence Act et le Personnal Data Privacy and Security Act, de 2005.

incrimination viserait l'usurpation de l'identité d'un particulier, d'une entreprise ou d'une autorité publique, ce qui inclut donc également le *phishing*. Si cette proposition n'a à ce jour pas rencontré le succès qu'elle mérite, ses dispositions ont quand même été reprises dans le cadre du plan de lutte contre la cybercriminalité, présenté par la Ministre de la Défense en février dernier. De ce fait, l'usurpation d'identité devrait être prochainement érigé en délit autonome, passible d'un an d'emprisonnement et de 15 000 euros d'amendes, dans la future loi de Programmation et de Performance pour la Sécurité Intérieure[81]. Cette nouvelle avancée permet de relever le renforcement du droit au respect de l'identité, ainsi que le lien entre ses dimensions réelle et virtuelle. Reste encore à en définir les contours avec précisions, afin de ne pas "trop" élargir le champ de l'usurpation tout en laissant au juge une marge suffisante d'interprétation et d'adaptation aux pratiques induites par les nouvelles technologies[82].

Au final, si l'identité virtualisée devait être la plus respectueuse de l'identité réelle, elle en reste pourtant bien loin, constituant même la source d'une multitude d'abus. Il reste à examiner l'identité immatérielle, fabrication pure et simple d'une personne n'ayant d'existence que dans le monde virtuel.

2. L'identité immatérielle fantasmée mais rattachée à l'identité réelle

Nous en arrivons au point où l'identité virtuelle n'a plus de référent dans la réalité.

L'identité immatérielle tend vers l'absolu. Nous prendrons pour cadre les jeux de rôle en ligne massivement multijoueurs (MMOG), annoncés dans l'introduction. Ces jeux reposent sur les contributions de milliers de personnes, qui peuvent être toutes connectées en même temps. De plus, le monde virtuel persiste même lorsqu'ils n'y sont pas présents. La communauté des joueurs développe des échanges qui peuvent être culturels ou économiques. Le jeu Second Life, qui est un des plus célèbres, est basé sur le principe d'une "seconde vie", comme son nom l'indique. De manière générale, des pratiques élémentaires de la vie réelle y sont reproduites, avec l'objectif de se rapprocher au maximum de celle-ci[83].

L'identité y est plus que jamais nécessaire, au même titre que dans la vie réelle, avec laquelle elle persiste à entretenir des liens très ambigus (a). La qualification même de cette identité pourrait se résoudre à être juridiquement immatérielle (b).

---

[81] Intervention de M. ALLIOT-MARIE au Forum International de la Cybercriminalité, 20 mars 2008, disponible sur le site du Ministère de l'Intérieur, http://www.interieur.gouv.fr.

[82] MATTHOS F. J., "La création d'un délit d'usurpation d'identité sur Internet", *Gaz. Pal.*, 25 juillet 2008, pp. 6-9.

[83] SCARAMOZZINO Y.-E., *Les jeux en ligne – Du virtuel au réel*, Dossier Scaraye n° 2, 1ère partie, juillet 2006, Paris, p. 2, www.scaraye.com

a) La virtualisation hypocrite de l'identité immatérielle

L'identité se "matérialise" avec ce qu'on appelle l'avatar de jeu vidéo, dont le statut fait l'objet de nombreuses discussions[84]. Personnage entièrement virtuel, il permet au joueur d'évoluer dans l'univers de jeu interactif, et de communiquer avec d'autres avatars.

La principale caractéristique qu'on doit lui reconnaître est l'absence de lien avec une personne réelle, hormis le joueur. On doit entendre par là que les traits d'identité de l'avatar sont absolument imaginaires, et ne se réfèrent à aucun individu du monde réel. Sa nature le conduit cependant à se rapprocher le plus possible d'une personne réelle, comme tout personnage protégé au titre de la propriété littéraire et artistique[85]. Ce rapprochement augmente la crédibilité du monde virtuel et l'intérêt de l'utilisateur qui y évolue[86]. Si on s'en tient à Second Life, le personnage peut être doté d'un physique, d'une garde-robe, d'un domicile, une profession, de relations amicales, professionnelles… Il peut être propriétaire, locataire, salarié, chef d'entreprise, vendeur, acheteur… L'identité de l'avatar pourra varier selon le contexte du jeu, et l'objectif de celui-ci. Certains jeux vont bien plus loin dans le virtuel et constituent des univers purement fantastiques ou féeriques.

L'intérêt pour le joueur subsiste avec la personnalisation de son avatar, double virtuel idéalisé, figurant les fantasmes de la personne réelle et son désir d'évasion. Le réalisme va jusqu'à lui permettre de créer des objets, grâce à des logiciels de modélisation 3D, et de les vendre, non seulement dans le monde virtuel, mais aussi sur des sites de vente aux enchères… réelles ! Un véritable commerce d'objets virtuels s'est ainsi développé, représentant un grand intérêt pour les éditeurs de jeux et pour les joueurs. Un taux de change a même été établi dans certains jeux, entre la monnaie virtuelle et le dollar[87]. Les sommes échangées sont astronomiques[88] ; des plaintes pour vol ont déjà été enregistrées[89].

Le lien avec la réalité réapparaît malgré tout : l'avatar va contracter des droits et obligations pouvant impliquer une somme d'argent réel. Les contrats qu'il passe dans le monde virtuel sont exécutés dans le monde réel. Ces deux mondes ne cessent donc d'interagir. Comment considérer l'identité de l'avatar au sein de cet imbroglio ? Peut-on lui reconnaître une valeur juridique ? Des arguments ont déjà été avancés, tendant à lui reconnaître un droit à l'image, un droit à l'intégrité, ce qui tend à lui conférer une protection juridique. De même, en tant que vendeur ou acheteur, il se trouve partie à un contrat. Son action produit donc des normes juridiques, ce qui peut en faire

---

[84] CIPRUT M., "Quel statut juridique reconnaître à l'avatar ?", *Les Échos*, jeudi 10 janvier 2008, p. 30.
[85] EDELMAN B., "Le personnage et son double", *D.*, 1980, Chronique, pp. 225-230 ;
[86] LÉVY Pierre, *op. cit.*, p. 95.
[87] CHÉRON A., "Un joueur de MMOG peut-il être créateur protégé juridiquement ?", 14 juin 2006, http://www.avocat-pla.com
[88] "Le Forum des droits sur Internet : à jeux virtuels, règles réelles", 27 novembre 2007, http://www/latribune.fr (un australien aurait ainsi acheté une île virtuelle pour près de 20 000€).
[89] SOUFFRON J.-B., "Droit des jeux vidéos : vols de biens virtuels dans des MMORPG", *Zdnet.fr*, 5 février 2008, http://www.zdnet.fr

un sujet de droit. En tant que tel, son existence juridique peut déjà être reconnue par les règles autonomes dont se dotent les univers dans lesquels il évolue.

La question va encore plus loin lorsque des joueurs portent plainte suite au "cyber-viol" de leur avatar. Faut-il reconnaître une telle incrimination en droit pénal[90] ? L'identification de la personne réelle à la personne immatérielle doit-elle être légitimée à ce point ? Le choc peut en effet être dur pour le joueur.

L'identité de l'avatar doit-elle alors être reconnue dans l'univers juridique de la réalité ? La réponse semble évidemment négative.

b) L'inexistence juridique de l'identité immatérielle : véritable virtualité ?

L'identité de l'avatar ne saurait être reconnue par le droit positif, dont l'application se fait dans le monde réel, pour des personnes réelles. Il ne saurait donc être traité comme tel, même s'il peut quand même être protégé à un autre titre.

En effet, les seuls arguments permettant de reconnaître à l'avatar un droit à l'intégrité sont rattachés à la propriété littéraire et artistique, et non aux droits de la personnalité. La protection lui sera garantie par le droit moral, et c'est son auteur qui aura la charge de l'exercer. Le lien avec la réalité reste indéniable, ne serait-ce qu'à ce niveau. Si l'avatar a une identité, c'est uniquement en tant que personnage de fiction, et la protection ne pourra être accordée que sur ce fondement. Sa nature particulière, évolutive, vient quand même bouleverser la propriété intellectuelle au niveau du concept de personnage, ce qui jette aussi le trouble sur le titulaire des droits de propriété intellectuelle[91]. Cette nature le rapproche de plus en plus de la réalité, au point de rappeler l'état des personnes réelles.

Mais c'est aussi à ce niveau que la reconnaissance de son identité ne peut être acceptée. Elle supposerait de distinguer entre des personnes corporelles et des personnes incorporelles (qui ne seraient pas des personnes morales) ce qui juridiquement paraît aberrant. Quand bien même l'idée d'une personnalité virtuelle a été envisagée en matière informatique[92], ce n'est qu'en considération d'une intelligence autonome et artificielle. Or l'avatar, si développé, intègre et réaliste soit-il, reste sous le contrôle d'une personne physique. Il n'a aucune autonomie de la volonté, aucune intelligence propre. Il n'est que l'émanation d'une personnalité réelle[93], quand bien même celle-ci serait totalement différente. De plus, ses facultés d'action sont très largement

---

[90] CHARBONNIER M.-E., "Un nouveau concept : le cyber-viol virtuel", *AJDP*, juillet 2008, p. 295.

[91] VAN DEN BULK P., "Le régime juridique des avatars créés dans le cadre des jeux vidéo – premières réflexions", *PI*, juillet 2007, pp. 279-284.

[92] CAPRIOLI E., "Consentement et systèmes informatiques", *Droit et intelligence artificielle – Une révolution de la connaissance juridique*(ss la dir. de BOURCIER D., HASSETT P. et ROQUILLY C.), Romillat, Collection Droit et technologies, Paris, 2000, p. 125.

[93] Recommandation "jeux vidéo en ligne : quelle gouvernance ?", *Forum des droits sur l'Internet*, 9 novembre 2007, p. 46, http://www.foruminternet.org

limitées par les contraintes techniques du logiciel. Le monde virtuel ne peut reproduire la réalité avec toute l'incertitude qui la caractérise.

Il serait tout aussi absurde d'affirmer que l'avatar est mandataire de la personne qui le contrôle, puisque c'est elle qui s'engagera, tout simplement en cliquant sur sa souris ou son clavier. Il représente au mieux un intermédiaire technique, protégeable au titre du droit d'auteur, et indissociable de la personne qui le contrôle.

Il est vrai toutefois que les pistes sont brouillées par un dangereux rapprochement de la réalité. Il serait plus simple de distinguer nettement monde réel et monde virtuel d'un point de vue juridique, afin d'anéantir toute interaction entre les deux. Le droit commun n'aurait pas à s'appliquer pour des actes du monde virtuel, impliquant notamment une monnaie virtuelle. Inversement, les règles fixées et développées par les avatars (joueurs) dans le metavers auraient un champ d'application bien délimité. Le droit pourrait aussi être totalement virtualisé dans ces univers, avec le développement d'une vraie cyber-justice pour régler les litiges qui y surviennent. La distinction, encore recherchée[94], entre les actes relevant de l'un ou de l'autre serait tout simplement établie. L'identité immatérielle prendrait alors sa vraie signification, en étant reconnue dans les seules limites du monde virtuel, tout en respectant l'esprit ludique du jeu en cause. Le qualificatif de virtuel serait entendu dans son sens le plus absolu.

Mais même dans ce cas-là, l'interaction avec la réalité et les risques d'atteinte sont toujours possibles. En effet, au même titre que les réseaux sociaux, un avatar peut permettre d'usurper l'identité de quelqu'un, d'en trahir l'intégrité, de dissimuler une autre personne. La question même du droit à l'image se pose déjà si les moyens techniques permettent de redessiner avec précision le visage d'une personne réelle. La reproduction qui en serait faite porte indubitablement atteinte à cette dernière, si elle ne l'a pas autorisée. L'ensemble des dispositions que nous avons évoquées au niveau de l'identité virtualisée sera alors applicable, puisque nous repassons dans cette seconde dimension. La classification même que nous avons retenue se heurte à une grande perméabilité des notions.

Tout cela permet de réaffirmer la nécessité de dégager un droit au respect de l'identité, tant celle-ci se trouve au cœur du cyberpesace.

Les progrès techniques ne cessent de renouveler l'appréhension juridique de l'être humain[95]. Les nouvelles technologies de l'information et de la communication connaissent une évolution globale, rapide, incessante, imprévisible, affectant positivement ou négativement les individus[96]. Au niveau du cyberespace, elles induisent un double processus à l'égard des personnes.

Tout d'abord, elles ont fourni au plus grand nombre des techniques d'artifice assurant une liberté d'expression sans limite. Le processus peut être envisagé du point de vue de la création artistique. Tout un chacun peut

---

[94] MALKA M., "Le droit dans Second Life", *Cyberlex*, 17 avril 2008, http://www.cyberlex.org
[95] DOUAY S., "L'identité personnelle dans la civilisation de réseaux", *D.*, 2007, p. 2623.
[96] FRAYSSINET J., "Droit, droits et nouvelles technologies", *op. cit.*, p. 1.

maintenant écrire, dessiner, photographier, filmer, monter… en bref, créer en toute liberté et à un moindre coût. Le public devient lui-même créateur dans un processus d'auto émulation. De fait, et c'est là la deuxième tension, il devient aussi objet de sa propre création. Tout un chacun est aussi photographié, commenté, filmé, monté, déformé… en bref, reçu et disséqué en toute liberté par le public dont il fait partie. Le procès du cinéma initié par Walter Benjamin dans les années trente[97] trouve ici un écho remarquable. À l'instar de la caméra qui décompose tout mouvement de l'acteur (objet) avec la force du détail, les nouvelles technologies décomposent les individus (acteurs) et révèlent leur intégrité. Le tout se fait dans une "mise en scène" numérique, aussi artificielle qu'une œuvre d'art, auto-générée de façon aléatoire et sans but prédéfini ; le cyberespace représente ainsi "l'universel sans totalité"[98].

Les êtres humains y sont devenus des objets virtuels, formant la matière de cette mise en scène. Celle-ci, constamment renouvelée, exige des individus qu'ils se dévoilent et se livrent toujours plus au spectacle public. L'identité personnelle, qui fait l'unicité de la personne, qui fait qu'il se sent lui-même, échappe à son propre titulaire dans le monde virtuel. Elle est déjà découpée en au moins deux dimensions, numérique et virtualisée, aux caractéristiques bien distinctes. Quoi de plus naturel que de se voiler pour échapper à cette perte de contrôle ? En profitant des moyens offerts par le cyberespace, l'identité peut aussi être imaginaire, immatérielle. Cela est d'autant plus légitime que cette fabrication nourrit le processus de création. L'identité virtuelle constitue donc un objet multiforme, jetable, modulable, réutilisable, plurielle… elle n'est plus l'identité d'un être humain, bien qu'elle ne puisse s'en détacher totalement.

La tension nouvelle entre l'unification et la réification de l'identité personnelle dans le cyberespace justifie le renouvellement et l'adaptation du Droit dans le but de concilier ces logiques opposées. Cette innovation révèle les évolutions de la notion d'identité personnelle, et nous ramène au niveau du droit au respect de l'identité[99]. De façon logique, il est essentiel que toute personne puisse contrôler l'usage qui est fait de son identité. Nous avons vu comment le droit positif offre déjà de nombreux moyens pour préserver le lien entre la personne et la projection juridique de son identité. La philosophie des textes tend toujours à faire primer le respect de l'identité personnelle, et les dispositions à venir ne feront que le confirmer. L'existence du droit au respect de l'identité, déjà visé par certaines législations en tant qu'*habeas data*, comme nous l'avons vu, apparaît implicitement au travers de ces textes. Ces derniers protègent déjà, de différentes manières, les composants de l'identité contre toute utilisation qui en est faite. Le droit à l'image et l'action en contestation de nom en sont des illustrations.

---

[97] BENJAMIN W., *L'œuvre d'art à l'époque de sa reproductibilité technique*, Allia, Paris, 2007, 80p. (édition originale : 1935).
[98] LÉVY P., *op. cit.*, pp. 129-159, pour de plus amples développements sur ce concept.
[99] MARINO L., "Les nouveaux territoires des droits de la personnalité", *Gaz. Pal.*, 19 mai 2007, p. 1483.

Il importerait pourtant de consacrer ce droit à l'identité de façon autonome, comme nouveau droit de la personnalité. L'identité personnelle serait détachée des fondements auxquels on la rattache trop souvent, et qui ne sont que ses éléments constitutifs : la vie privée, la liberté individuelle[100] et la dignité. Alors que la biométrie individualise toujours plus les personnes, celles-ci doivent être assurées du respect de leur identité, que son environnement soit naturel ou virtuel. Le Droit se doit d'intégrer ces deux dimensions de la façon la plus simple possible. La reconnaissance de ce droit à l'identité aurait le double avantage de la simplicité et de l'efficacité. Elle assurerait l'intégrité de la personne dans les deux environnements auxquels l'être humain a accès. Ainsi le Droit intègrerait-il le nouvel espace-temps de nature immatérielle[101] qu'induit le cyberespace.

Reste à souhaiter que cette dualité soit maintenue, et que le monde virtuel ne devienne pas la seule réalité des individus.

[100] BIOY X., *op. cit.*, p. 75.
[101] FRAYSSINET J., "Droit, droits et nouvelles technologies", op. cit., pp. 2-3.