

# Personne et droit entre micro- et nanotechnologies. Opportunité ou insécurité ?

Silvia Visciano

Adresse de l'auteur Silvia.Visciano@malix.univ-paris1.fr

**Résumé :** La présente communication vise essentiellement à proposer une brève mise en question de certains dilemmes éthiques et de droit posés par les nouvelles technologies à taille micro et nano. Les questions sont multiples et l'ambivalence et le paradoxe que nous trouvons déjà au sein des technologies d'information et de communications deviennent complexes au fur et à mesure que les technologies se miniaturisent. Telles sont les enjeux que nous voudrions discuter ici au moyen d'un droit positif encore gestant et par le biais descriptif de certains objets concrets : les étiquettes RFIDs Une timide référence aux puces ADN nous permettra en fin de nous ouvrir à la problématique toute nouvelle et irrésolue des nanobiotech.

**Summary :** Our contribution is intended in purposing a brief presentation of some ethical and juridical problems posed by new micro and nanotechnologies. The questions are multiple, the ambivalence and the paroxysm already existing for some information and communication technologies become more complex with the miniaturising of technological objects. The use of an 'in-the-making right' and some concrete objects for completing - RFid tags will help this general evaluation. Finally, a reference to DNA chips will be useful for beginning the description of some nanobiotech questions.

**Riassunto :** Il nostro contributo intende proporre essenzialmente una breve tematizzazione di alcuni dilemmi etici e di diritto posti dalle nuove tecnologie di taglia micro e nano. Le questioni sono multiple e l'ambivalenza, perfino il parossismo, già presenti in seno a talune tecnologie dell'informazione e della comunicazione si fanno complessi nella misura della progressiva miniaturizzazione degli oggetti di tecnologia. Tali sono le problematiche che intendiamo discutere in questa sede a mezzo di un diritto ancora in gestazione e secondo l'ipotesi descrittiva delle etichette RFid. Infine, un breve sguardo ai chip DNA ci permetterà di inquadrare in prospettiva la problematica concernente il nanobiotech.

**Mots clés :** Microtechnologies, nanotechnologies, RFID, personne, données personnelles, puces ADN.

**Key-words :** Microtechnologies, nanotechnologies, RFID, person, personal data, DNA chips.

**Parole chiave :** Microtecnologie, nanotecnologie, RIId, dati personali, chip DNA.

# 1. Introduction

Les micro- et les nanotechnologies constituent un « secteur stratégique de recherches en croissance rapide, avec un potentiel de développement économique remarquable dans plusieurs domaines » [Programme National Nanosciences ; <http://www.nanomicro.recherche.gouv.fr/>] : l'informatique, l'optique, les télécommunications, la biométrie, la chimie, la médecine, la cognition y sont engagées et intéressées<sup>1</sup>.

Dans ce cadre, et plus spécifiquement, la filière électronique - nous pensons notamment à l'électromécanique et à la bioélectronique - est déjà une réalité.

Comme a pu l'affirmer Mme Viviane REDING, membre de la Commission chargé de la société de l'information et des médias, « qu'il s'agisse des interphones de surveillance, des télécommandes de porte de garage, des alarmes ou des implants médicaux », les dispositifs sans fils concernent désormais nous tous<sup>2</sup>. En effet, les implants, hors ou dans le corps humain, et tous les outils rassemblant des informations sur la personne - qu'ils soient de taille micro- ou nanométrique - laissent présager des évolutions importantes dans plusieurs domaines : juridique, anthropologique, économique, éthique, sociale.

Tout ceci nous oblige à voir la personne comme le point de rattachement et de rencontre d'accessoires corporels et immatériels et nous invite à prendre en considération, aujourd'hui plus qu'hier, à la fois les divers avantages et les risques liés tant à la personne elle-même qu'aux autres personnes, physiques ou morales, avec lesquelles elle est en relation. De ce fait, la personne et les réseaux dans lesquels elle interagit sont impliqués par l'évolution des techniques, que ce soit au niveau individuel ou collectif.

Ceci souligné, il faut investiguer continuellement la relation existant entre sujet-personne et objet technologique. De plus, en tant que juristes, il nous faut relever en amont la complexité constitutive de la personne juridique. A la fois sujet de droits, source et destinataire de valeurs et de principes inhérents, elle acquiert progressivement une dimension technico-symbolique tout en préservant sa qualité intangible. Comme le dit magistralement Mme Catherine LABRUSSE-RIOU, il nous faut alors rechercher des outils juridiques pouvant prendre en charge la nature humaine et tout « ce qu'il y a d'indémontrable dans ce qui nous fait vivre, humainement, l'exigence de liberté et de dignité, l'indivisibilité du corps et de la personne » [Labrusse-Riou 2007].

Si la qualification de personne déclenche en général la sauvegarde de valeurs et de libertés, impute des obligations et attribue des droits, si « le corps humain dans sa globalité [est] fort bien protégé car il se confond avec la personne objet de toutes les faveurs du droit » [Hermitte 88] les données personnelles - biométriques, informatiques, génétiques -, côté immatériel et bien biographique prodigieux, témoignent sa vulnérabilité, les risques de son appréhension et de son appropriation. A leur tour, l'appréhension et l'appropriation relèvent

---

<sup>1</sup> Dans sa communication *Vers une stratégie européenne en faveur des nanotechnologies* (COM(2004) 338) la Commission UE a émis en 2004 des recommandations et des propositions visant à stimuler la recherche et le développement sur les nanotechnologies en Europe. Une consultation publique sur la communication, organisée entre août et octobre 2004, avait aussi démontré l'effervescence du secteur : on voyait bien un impact sur l'industrie européenne et ses citoyens dans les années à venir (cf. Rapport Nanoforum, décembre 2004). Le 7 juin 2005, la Commission a adopté un plan d'action pour l'Europe 2005-2009 définissant des mesures pour la mise en oeuvre immédiate d'une stratégie de N&N (Nanosciences et Nanotechnologies) « sûre, intégrée et responsable » (COM(2005) 243 final).

<sup>2</sup> Cfr. *Des alarmes aux implants médicaux: la Commission libère des fréquences dans l'UE pour les dispositifs sans fil à courte portée*, doc. n. IP/06/1808, Bruxelles, 14 décembre 2006. En ce qui concerne la France, rappelons qu'une décision du 25 juillet 2006 (n. 06-0841), homologuée par un arrêté du 6 septembre 2006 (J.O n° 212 du 13 septembre 2006, p. 13475), a permis à l'ARCEP (Autorité de régulation des télécoms), de fixer les conditions d'utilisation des fréquences radioélectriques pour les applications d'identification par radiofréquences.

d'une part de la montée en puissance technologique du sujet voulant maîtriser l'autre par le biais de certains objets micro- ou nanotechnologiques, d'autre part des incertitudes qui continuent à régner sur la notion de personne et ses rapports avec ses informations personnelles.

## 2. La personne à l'épreuve du micro e du nano

Au sujet de certaines microtechnologies, un « grand intérêt à la trace » [Pedrot 03] des personnes est retrouvé et une crainte majeure est exprimée au sujet de la vigilance<sup>3</sup>: opportunité et insécurité se relient autour de la personne. Pouvant d'une part gérer en plein confort son quotidien - nous pensons à la gestion automatique de droits numériques, à la connexion Internet sans fil, à l'identification par radio-fréquence -, d'autre part elle est laissée démunie, organisée de l'extérieur, suivie, souvent enregistrée et évaluée par ses mouvements, par les données qu'elle dissémine. Ainsi elle abdique plus ou moins consciemment à son intimité, à l'intégrité de sa personnalité réelle et virtuelle, à sa liberté individuelle en faveur d'une recrudescence des moyens de surveillance.

De son côté, le nano franchit aujourd'hui les frontières entre les disciplines formelles de la biologie, de la chimie et de la physique. En effet, si l'on peut observer, manipuler, simuler des briques du vivant, on peut aussi inventer de nouvelles structures tout en travaillant sur l'inanimé, l'inerte: c'est le champ ouvert par les nanobiotechnologies<sup>4</sup>.

Les composants électroniques (micro et nano) et le domaine des nanobiotechnologies relancent donc avec vigueur deux questions juridiques différentes :

- la ***relation de la personne avec ses attributs en général et ses données en particulier***. A ce propos il nous convient de rappeler que l'article 9 du code civil français énonce que « chacun a droit au respect de sa vie privée »<sup>5</sup>, ainsi laissant à l'interprétation audace, souvent astucieuse de la jurisprudence le devoir d'interprétation, d'éclaircissement, d'élargissement de ses contenus et l'application de l'article 1382 en matière de responsabilité civile aux cas d'espèces (nous pensons notamment aux

---

<sup>3</sup> Cf. à ce propos, MURAKAMI WOOD D., *Report on the Surveillance Society for the Information Commissioner by the Surveillance Studies Network*, 09.2006. Le rapport part du constat suivant : "To think in terms of surveillance society is to choose an angle of vision, a way of seeing our contemporary world. [...] It is not just that CCTV may capture our image several hundred times a day, that check-out clerks want to see our loyalty cards in the supermarket or that we need a coded access card to get into the office in the morning. It is that these systems represent a basic, complex infrastructure which assumes that gathering and processing personal data is vital to contemporary living" (p. 3). Cette affirmation met bien en évidence le fait que la connectivité est aujourd'hui généralisée et qu'elle s'adresse progressivement à la fois à l'interconnexion et à une diffusion désordonnée.

<sup>4</sup> Au-delà des aspects environnementaux ou sanitaires, les micro- et nanotechnologies portent sur l'intégrité personnelle et sur la protection de la vie privée. Nous avons pu le constater lors de l'école de organisée par le Comité d'éthique du CNRS *Entre liberté et responsabilité : La recherche en nanosciences et en nanotechnologies* (5-7 mars 2007, Centre de Physique des Houches). Les conférenciers ont illustré les avancées technologiques (objets intelligents/Internet des choses ; laboratoires sur puces ; vecteurs des médicaments, puces ADN, Réseaux de nano-senseurs sans fils, etc.) et ont souligné à maintes reprises l'impact du nano tant sur les technologies de l'information que sur les développements dans le domaine biologique.

<sup>5</sup> J.-C. SAINT-PAU a défini le contenu de cet article une véritable « matrice des droits de la personnalité » (cf. note sous Cass. Ire civ., 16 juill. 1998, D. 1999, Jur. p. 541). Au niveau international et communautaire voir aussi la Déclaration Universelle des Droits de l'Homme (art. 12), Pacte international relatif aux droits civils et politiques (art. 17), la Convention Européenne de Sauvegarde des Droits de l'Homme et des libertés fondamentales (art. 8), la Déclaration universelle sur la bioéthique et les droits de l'homme (art. 9), la Charte Européenne des Droits Fondamentaux (art. 7).

atteintes à l'image, à la voix, au domicile de la personne par le biais de la géolocalisation, des dispositifs de vidéosurveillance, des instruments biométriques). De leur côté, les renseignements personnels sont disciplinés en France par la loi « *Informatique, fichiers et libertés* » du 6 janvier 1978, modifiée par la loi n. 2004-801 du 6 août 2004, relative à la protection des personnes physiques à l'égard des données à caractère personnel. Le décret d'application de la nouvelle loi informatique et libertés a été adopté le 20 octobre 2005. En Italie le *Code en matière de protection des données personnelles* (d. lgs. 196/2003)<sup>6</sup> a modifié la loi préexistante n. 675 du 31.12.1996. La miniaturisation technologique dit toute de la difficulté de dire la « *Forme sujet de droit* » [Edelman 99] - corps réel et corps électronique [Rodotà 06], matérialité et immatérialité - dans le langage du droit et montrent l'intérêt croissant de divers sujets (l'Etat, les associations, les entreprises privées, les syndicats, etc., qu'il s'agisse de gouvernants ou de gouvernés) à l'appréhension des informations personnelles remises volontairement ou laissées involontairement par le sujet pour des finalités - lucratives ou non-lucratives - de marketing, statistiques, de sécurité, de vigilance, et même pour des buts illicites. Ceci ne relève plus seulement des fonctions traditionnelles du droit - protection des individus, sauvegarde des liens sociaux, maintien de la paix sociale, certitude -, mais démontre qu'un rapport marchand demeure sous-jacent au geste d'« *entretien de ce corps* » [Strickler 06] en principe hors commerce avec tous ses éléments corporels ou saisissables par identification ;

- le ***rapport du corps humain avec les enjeux biotechnologiques***. Ce rapport est aussi traditionnel que les craintes de normalisation de l'être humain<sup>7</sup>. Le droit qui assume depuis longtemps un rôle descriptif et prescriptif n'est tout simplement pas en mesure de singer le temps des progrès scientifiques et technologiques - tout particulièrement biomédicales et biotechnologiques - harmonisés aux exigences d'expérimentation, aussi bien que de thérapie, de démantèlement, de parcellisation et de fabrication. Si l'art. 16-3 du Code civil français garantit la sauvegarde de l'intégrité humaine<sup>8</sup>, si le droit pénal reconnaît le principe du *nolli me tangere*, ainsi traduisant en conception juridique de la personne le caractère inviolable de la nature humaine, le droit fait face encore aujourd'hui à certains libéralismes élaborés en médecine depuis le XIXème

<sup>6</sup> Le commun dénominateur juridique des deux Pays considérés est la Directive 95/46/CE du Parlement européen et du Conseil, 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. Cette directive distingue les données qui permettent une identification directe de celles qui autorisent l'identification indirecte. L'art. 2 énonce ainsi qu'« on entend par données à caractère personnel toute information concernant une personne physique identifiée ou identifiable, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale ». Si l'identification directe des personnes passe par leur nom et leur localisation, l'univocité identificatoire passe aujourd'hui de plus en plus par le regroupement et le recoupement des codes et de numéros qui lui sont attribués (numéro de sécurité sociale, code fiscal, cartes bancaires, etc.).

<sup>7</sup> Le *recto* du désir normalisateur aurait son *verso* dans le « défaut de conformité » de l'homme (cf. LEGROS E. Z., L'embryon défectueux, PA 2002, n. 243, p. 63 ss.).

<sup>8</sup> « Il ne peut être porté atteinte à l'intégrité du corps humain qu'en cas de nécessité médicale pour la personne ou à titre exceptionnel dans l'intérêt thérapeutique d'autrui. Le consentement de l'intéressé doit être recueilli préalablement hors le cas où son état rend nécessaire une intervention thérapeutique à laquelle il n'est pas à même de consentir ». Le 1<sup>er</sup> alinéa de l'art. 16-4 continue en soulignant que « nul ne peut porter atteinte à l'intégrité de l'espèce humaine ». De plus, les articles 16 et 16-1 assurent le respect du corps humain et à son inviolabilité. Introduits en France par les lois de bioéthique de 1994 (révisonnées en 2004), les articles semblent donc constituer la nature extrapatrimoniale du corps. J CARBONNIER avait déjà souligné à ce propos que « le corps humain est le substratum de la personne [...] De ce qu'il est la personne même, le corps tire une place tout à fait particulière dans le droit » (CARBONNIER J., *Droit civil. Les personnes*, Paris, 2000, vol. 4, p. 243 ss).

siècle et aiguisés par les dernières technosciences [Edelman 99]. Déjà en 1932 L. Josserand écrivait : « entre le patrimoine et la personne humaine [...] des points de contact s'établissent, de plus en plus nombreux ; ces deux concepts antithétiques voisinent volontiers et, dans cette fréquentation, la personne humaine laisse un peu de son intégrité et de son intangibilité [...] descendue du piédestal où l'avait hissé la déclaration des Droits de l'homme et le code civil de 1804, elle devient volontiers matière à transactions, à abandons, à réparations, à combinaisons » [Josserand 32]. Puisqu'elles sont transformées, les ressources corporelles (génétiques, organiques, etc.) ont tendance à sortir de leur configuration indisponible et non-patrimoniale absolue pour se qualifier de l'accessible. Mais le droit, quant à lui, doit pouvoir continuer sa vocation procédant « d'un discours ou d'un image pour mener au non-dit, à l'invisible » [Labrusse-Riou 95] au travers des fictions, de la technique juridique et bien avant d'une fonction anthropologique. Cet approche qui ne peut faire l'illégitimité du discours biologique pur, peut néanmoins offrir une alternative à certaines tentations réductionnistes si bien qu'à la logique du calcul et de la prédiction à tout prix.

La présente communication vise essentiellement à proposer, dans ce domaine à évolution rapide, une brève mise en question des dilemmes éthiques et de droit posés par les nouvelles technologies à taille micro et nano. En effet « s'ils peuvent être utilisés pour pallier la déficience de certaines fonctions corporelles, [les objets et les implants micro- et nanométriques] peuvent aussi être source d'abus, notamment lorsqu'il est possible d'y accéder par réseau informatique » [Groupe européen d'éthique des sciences et des nouvelles technologies 05] ou par le biais de la biologie<sup>9</sup>. Bien que, selon certains, ils sont en mesure de restaurer des capacités fonctionnelles endommagées, contribuant ainsi à la promotion de la personne et de sa dignité humaine, la considération qu'ils représentent un risque pour celle-ci peut aussi bien être envisagée [cf. Dupuy 02, Bensaude-Vincent 04].

Un débat nécessaire, même attendu sur ce un sujet si surabondant, demande au juriste une posture argumentative ciblée, lui permettant de revenir à sa vocation primaire, celle de prendre en considération et d'analyser les règles. Il s'agit donc au préalable de considérer des objets singuliers et spécifiques ; après il faut vérifier si les catégories juridiques dont le droit se munit aujourd'hui sont valables pour ceux-ci, pour essayer en fin une réponse normative tentant compte d'une analyse aussi bien politique.

Telles sont les enjeux que nous voudrions discuter ici au moyen d'un droit positif encore gestant et par le biais descriptif d'objets concrets : les étiquettes RFIDs. Une référence aux puces ADN nous permettra en fin de nous ouvrir à la problématique toute nouvelle et irrésolue des nanobiotech.

---

<sup>9</sup> Comme l'affirme M. Ph. LEMOINE, une dissimulation de la complexité des « interfaces intuitives » est souhaitable et peut être réalisée par des « alertes intuitives » visant des personnes « entraînés à détecter rapidement les pièges et les glissements qui peuvent résulter de technologies apparemment anodines » (cf. la Tribune CNIL - Commission Nationale de l'Informatique et des Libertés - du 20.11.2003).

## 2.1 Les RFIDs

La technologie RFID (*Radio Frequency IDentification*)<sup>10</sup> permet l'utilisation d'une fréquence radio pour identifier automatiquement un objet ou une personne. Héritières du traditionnel code à barre, les puces électroniques miniatures (dites transpondeurs, étiquettes, ou tags) utilisant cette technologie se constituent d'un microprocesseur et d'une antenne bobinée ou imprimée, et s'associent à un ou plusieurs lecteurs (circuits électroniques composés eux-mêmes d'une carte électronique et d'une antenne pouvant participer activement à l'automatisation des processus et pouvant être portatifs) communiquant par voie électromagnétique. A son tour le champ électromagnétique sert tant de vecteur à l'information entre la puce et son lecteur qu'à fournir l'énergie d'activation des puces.

Les étiquettes représentent le support informationnel combinant le traitement du signal reçu et le stockage des données échangées. *Grosso modo*, nous pouvons affirmer que l'étiquette répond au signal lancé par le lecteur et lui permet la lecture, puis l'envoi des données encodées à un serveur qui traitera les informations reçues en la rapportant à une base de données construite ad hoc. L'envers est aussi possible, car l'étiquette est dans certaines conditions en mesure d'accéder aux données se trouvant dans le lecteur.

Le mode de fonctionnement des puce est en lecture seule ou en lecture et écriture. Fonctionnant en lecture seule, les *étiquettes passives* fonctionnent comme les codes à barres linéaires et sont programmées avec des données non modifiables. Certains dispositifs plus sophistiqués, reconnus comme *semi-passifs* (Radio-tags Read-Writes), peuvent dans ce cadre discerner certaines variations physiques. En ce qui concerne les *étiquettes actives*, elles peuvent être écrites et surécrites, effacées, modifiées et lues.

Les RFID ne se distinguent pas seulement par la voie *technologique*, mais aussi par celle *applicative*. Si certaines puces RFID sont utilisées pour le stockage des données relatives à des produits (il peut s'agir des applications de logistique pour suivre l'acheminement de marchandises), d'autres permettent l'accès aux lieux, l'abonnement aux transports publics (nous pensons à la carte Navigo de la Ratp) ou le péage automatique sur autoroute. Comme le dit bien Mme Gildas AVOINE « dans le premier cas, le but du protocole est d'obtenir l'identité de l'objet interrogé mais aucune preuve de cette identité n'est requise : c'est un protocole d'identification. [...] Dans le second cas, il est important qu'une preuve de l'identité soit fournie : c'est un protocole d'authentification. Par abus de langage, protocole RFID désigne aussi bien un protocole d'identification qu'un protocole d'authentification » [Avoine 06].

## 2.2. RFId et protection des données personnelles

Si le potentiel économique relatif à la technologie RFID est énorme et encore peu exploité au niveau communautaire - la stratégie UE lancée en matière le 15.03.2007 est assez

---

<sup>10</sup> Le système RFID est utilisé depuis la seconde guerre mondiale. Les militaires américains reconnaissaient ainsi à distance des avions « Friend or Foe ». Le premier brevet est apparu aux Etats-Unis en 1969. En Europe la technologie est arrivée en tant que moyen pour l'identification du bétail. A propos des usages que l'on fait dans le monde aujourd'hui, le cabinet britannique indépendant IDTechEx a présenté en janvier 2007 sa dernière étude portant sur 2 450 études de cas dans 92 pays met (<http://www.idtechex.com/products/en/articles/00000515.asp>; date de consultation : 06.06.2007). L'étude en question révèle un usage très diversifié des applications RFID : si l'Amérique du Nord est le premier utilisateur de puces RFID destinées aux biens de consommation et au commerce de détail, l'Europe utilise beaucoup cette technologie dans les secteurs de la finance et de la sécurité. Au contraire l'Asie australe opte à la fois pour le taggage unitaire et pour l'identification des personnes, permise par une certaine permissivité législative.

prédictive là-dessous<sup>11</sup> - sous un point de vue strictement juridique, nous constatons que l'utilisation de certaines puces RFID peut ainsi engendrer des types différents de risques juridiques qui ne se limitent pas à la problématique de la protection des données personnelles et au maintien de leur caractère confidentiel : « la capacité de collecter subrepticement tout un ensemble de données sur une seule et même personne, de tracer les gens lorsqu'ils se déplacent dans des espaces publics (aéroports, gares, magasins), de perfectionner des profils grâce à la surveillance des comportements des clients dans les magasins, de lire les détails des habits et des accessoires portés ou des médicaments transportés par une personne »<sup>12</sup> constituent le sujet d'une préoccupation majeure en matière d'atteinte à la vie privée personnelle, à l'autodétermination, à la libre circulation des personnes, au principe d'inviolabilité du corps humain. La trace laissée par le sujet pourrait fournir d'abord le prétexte pour l'accès, le partage, la collecte, l'intégration d'informations, ensuite pour une pernicieuse pénétration au cœur de ses goûts, de ses tendances, de ses mouvements, de ses choix. Ce maillage d'informations avait déjà inquiété en 2003 les Commissaires à la protection des données et à la vie privée<sup>13</sup> et la CNIL<sup>14</sup>, et inquiète aujourd'hui les citoyens européens<sup>15</sup>, peut-être les mêmes qui s'étaient déclarée enthousiastes en matière 'nano'.

---

<sup>11</sup> V. la *Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions sur le thème L'identification par radiofréquence (RFID) en Europe: vers un cadre politique*, doc. n. SEC(2007) 312 ([http://ec.europa.eu/information\\_society/newsroom/cf/itemlongdetail.cfm?item\\_id=3247](http://ec.europa.eu/information_society/newsroom/cf/itemlongdetail.cfm?item_id=3247); date de consultation : 06.06.2007). En mars 2007 l'UE estimait en 43 les projets européens portant sur les technologies RFID. La Commission européenne soutient ces projets pour un chiffre de € 154 million sur une dépense totale de € 315 million. Nous rappelons aussi que la Commission a libéré en décembre 2006 des fréquences dans l'UE pour les dispositifs sans fil à courte portée. A ce propos cf. les Décisions d'harmonisation du spectre radioélectrique utilisé par les dispositifs à courte portée et les dispositifs d'identification par radiofréquence (RFID) dans la bande UHF (ultra haute fréquence) à partir de l'adresse [http://ec.europa.eu/information\\_society/policy/radio\\_spectrum/ref\\_documents/index\\_en.htm](http://ec.europa.eu/information_society/policy/radio_spectrum/ref_documents/index_en.htm) (date de consultation 06.06.2007). La Commission a accordé une dérogation demandée par la France en application de la décision 2006/804/CE en considération de « des justifications techniques suffisantes, fondées en particulier sur des études de compatibilité réalisées par l'Agence nationale des fréquences et la CEPT et tenant compte de facteurs de brouillage préjudiciable entre RFID et équipements militaires, notamment en ce qui concerne la puissance d'émission, la densité et les temps de cycles ».

<sup>12</sup> Article 29 - Groupe de travail protection des données, *Document de travail sur les questions de protection des données liées à la technologie RFID (radio-identification)*, 19.01.005, p. 2 (consultation à l'adresse [ec.europa.eu/justice\\_home/fsj/privacy/docs/wpdocs/2005/wp105\\_fr.pdf](http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp105_fr.pdf) Date de consultation : 06.06.2007).

<sup>13</sup> Lors de la Conférence internationale des commissaires à la protection des données et à la vie privée, tenue à Sydney en septembre 2003, la technologie RFID avait déjà fait l'objet d'une résolution concernant la nécessité de prendre en compte les principes de protection des données lorsque cette technologie se relie à des informations personnelles.

<sup>14</sup> L'article paru le 23.11.2003 sur le site débutait de la façon suivante : « La technologie de radio-identification (RFID) devient un enjeu économique majeur notamment dans les applications de la distribution et du transport. Du fait de leur dissémination massive, de la nature individuelle des identifiants de chacun des objets marqués, de leur caractère invisible, et des risques de profilage des individus, la CNIL considère que les RFIDs sont des identifiants personnels au sens de la loi Informatique et Libertés ». Lors d'une communication du 30.10.2003, M. Philippe LEMOINE, commissaire de la CNIL, avait individué en quatre pièges le danger d'une minorisation du « risque que présente cette technologie en matière de protection des données personnelles et de la vie privée ont été abordés : l'insignifiance (apparente) des données, la priorité donnée aux objets (en apparence toujours vis-à-vis des personnes), la logique de mondialisation (normalisation technologique basée sur un concept américain de « privacy » sans prise en compte des principes européens de protection de la vie privée) et le risque de « non vigilance » individuelle (présence et activation invisibles) » (<http://www.cnil.fr/index.php?id=1063>; date de consultation : 06.06.2007).

<sup>15</sup> La consultation publique lancée par la Commission de juillet à septembre 2006, à laquelle 2.190 sujets ont pris part, « a mis en évidence l'inquiétude de la population qui voit dans la RFID une technologie potentiellement envahissante. Des mesures appropriées de protection de la vie privée sont donc préconisées comme condition d'une large adhésion du public à la RFID. Les participants à la consultation en ligne pensent

A ce propos certaines outils existent déjà en droit communautaire : l'article 8 de la Charte des droits fondamentaux de l'Union européenne reconnaît le droit à la protection des données à caractère personnel. Ce droit fondamental est mis en œuvre dans le cadre juridique européen relatif à la protection des données à caractère personnel, qui comprend, outre que la directive 95/46/CE relative à la protection des données, la directive 2002/58/CE relative à la vie privée et aux communications électroniques et le règlement 45/2001 relatif aux traitements des données à caractère personnel par les institutions et organes communautaires. Certaines dispositions de fond reconnaissent des droits à la personne concernée et imposent des obligations au responsable du traitement des données. Des voies de recours adéquates en cas d'infraction et des mécanismes de contrôle sont aussi envisagés. Pourtant le *9ème Rapport annuel du Groupe Article 29 portant sur l'état de la protection des personnes à l'égard du traitement des données à caractère personnel dans l'Union européenne et les pays tiers*, adopté le 14.06.2006, soulignait encore qu'« aucuns redoutent que des entreprises et des gouvernements puissent utiliser la technologie RFID pour fouiller dans la vie privée des personnes. Le problème est aggravé par le fait que, en raison de son coût relativement faible, cette technologie sera à la portée non seulement d'acteurs de premier plan, mais aussi des intervenants moins importants et de simples citoyens » (p.14).

Quant à la France, la CNIL a considéré que les RFIDs peuvent contenir des données personnelles au sens de la loi Informatique et Libertés du 6 janvier 1978 modifiée par la loi du 6 août 2004, leur traitement devant ainsi répondre aux conditions fixées par cette loi : après l'expression du consentement un droit d'accès, de rectification des données erronées, même de suppression de ceux-ci est donc envisagé<sup>16</sup>. D'ailleurs l'art. 8 interdit de collecter et traiter des données sensibles : « 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 » ne sont pas stockables.

Les conditions de licéité du traitement des informations personnelles sont aussi strictement prévues. En particulier, au sens de l'art. 6 de la loi en question ces données - « adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et de leurs traitements ultérieurs, [...] exactes, complètes et, si nécessaire, mises à jour » - doivent être collectées et traitées de manière loyale et licite, pour des finalités déterminées, explicites et légitimes, sans qu'une modification ultérieure puisse être prévue en cas d'incompatibilité avec ces finalités.

De plus, si le système d'identification RFID implique l'usage d'un lecteur de puces collectant des données personnelles de façon directe ou bien indirecte, une obligation de déclaration à la CNIL subsiste. Par analogie il en va de même pour les autocommutateurs (cf. artt. 22-25). Le problème envisageable ici, et encore irrésolu aujourd'hui, demeure lié au sujet de l'obligation. Si la question ne se pose par rapport aux utilisateurs 'primaires' des données rendues accessibles et collectées par le moyen juridique du consentement de l'intéressé, les

---

que ces mesures résulteront des technologies de protection de la vie privée (70%) et d'actions de sensibilisation (67%); 55% envisagent une législation spécifique à la RFID comme la meilleure solution. En outre, pour ce qui est de savoir si les applications sociétales sont réellement bénéfiques, les avis sont partagés avec environ 40% de réponses positives et autant de réponses négatives » (*Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions sur le thème L'identification par radiofréquence (RFID) en Europe: vers un cadre politique*, cit., p. 6).

<sup>16</sup> Pourtant un problème inédit subsiste par rapport au pouvoir d'accès : comment peut le sujet intéressé accéder matériellement et de façon effective à ses données ? Si des dispositifs techniques tels que le système Dag (qui produit notamment des bracelets électroniques) garantissent la désactivation temporaire ou la neutralisation des puces RFID, ils ne sont pas encore répandus sur le marché. Le coût élevé de cette technologie 'corrective' empêche effectivement la pratique du droit en question.

utilisateurs 'secondaires'<sup>17</sup> ne sont pas toujours identifiables et joignables, c'est-à-dire que dans les faits ils ne sont pas tenus au respect de cette prévision de loi.

Le procès d'identification indirecte n'est donc pas suffisamment limité. Pire, le recoupement susceptible d'être opéré entre le contenu principal d'une puce et des données personnelles se trouvant sur un autre support - un passeport électronique, une carte de crédit, ou bien une carte de fidélité - n'est pas pris en considération par la loi<sup>18</sup>. Le fait de ne pas pouvoir retrouver à chaque instant la trace [Hermitte 03] laissée en amont de la chaîne informationnelle empêche dans les faits à la personne la mise à jour de son 'récit identitaire', donc la préservation du côté immatériel et insaisissable de son identité personnelle, pour autant qu'elle évolue et se modifie dans le temps. Les données risqueraient de ne pas être fidèles à la réalité. Une réalité qui est pourtant essentielle tant à la manifestation juridique de la personne et de ses rapports humains qu'à la fonction descriptive, qualificative et attributive du droit. D'ailleurs, l'intégrité des données personnelles renvoie directement et fait pleine foi de l'intégrité de la personne dont elles témoignent l'essence.

Ces questions juridiques montent et se font pressantes au fur et à mesure du développement de nouvelles architectures, de la conception, de la modélisation et de la mise sur marché de nouveaux circuits intégrés, de l'amélioration de l'interconnexion électronique et optique, de l'optimisation du transfert de l'information. Certes, les enjeux liés à la technologie RFID - lecture à travers le métal et conditions de propagation, miniaturisation et mémoire des puces, tenue mécanique, coût sur le marché/accès à la technologie, lecture à distance - laissent présager un très grand intérêt économique et social en la matière : une étiquette RFID qui originellement ne peut pas fonctionner sans son lecteur, sans un ordinateur et un système d'information, depuis un an est imaginée et observée dans des systèmes hybrides combinant plusieurs objets et modalités technologiques différentes<sup>19</sup>.

## 2.2 RFID : symboles et enjeux

Tout en délaissant la description de situations spécifiques d'utilisation des RFID telles que le placement sous surveillance électronique des travailleurs<sup>20</sup> ou bien celui des détenus

---

<sup>17</sup> La CNIL a récemment rappelé à tous les professionnels disposant de fichiers clients les règles s'appliquant au traitement des données bancaires (en mai 2007 la CNIL a vérifié le respect par un hôtel de ses obligations en matière de la gestion de ses fichiers clientèle et a relevé plusieurs manquements tels que le manque d'un protocole d'effacement des données enregistrées ou des renseignements à la clientèle).

<sup>18</sup> En Italie l' « Autorità garante per la protezione dei dati personali », organisme public de protection de données personnelles et de la vie privée, a approuvé un document portant sur les cartes de fidélité et sur les garanties des consommateurs (*'Fidelity card' e garanzie per i consumatori. Le regole del Garante per i programmi di fidelizzazione*, 24 février 2005, doc. web n. 1103045 <http://www.garanteprivacy.it/garante/doc.jsp?ID=1103045>). Ainsi elle a pu préciser les principes de nécessité et de proportionnalité qui doivent caractériser le service rendu. Au point 8 elle a souligné le fait que les données enregistrées pour des propos de marketing ou de profilage des consommateurs doivent être effacées respectivement après un an et deux ans.

<sup>19</sup> Nous pensons notamment au projet Hammer (*"Hand-held Apparatus for Mobile Mapping and Expedited Reporting"*) qui étudie un dispositif portable d'enquête mobile combinant le système GPS, la traditionnelle caméra, un lecteur d'étiquettes RFID pour détecter les traces archéologiques, ou bien pour intercepter les signes d'érosion architecturale ou urbanistique (cf. RFID Gazette, 12.07.2006 ; [http://www.rfidgazette.org/2006/07/innovation\\_in\\_h.html](http://www.rfidgazette.org/2006/07/innovation_in_h.html). Data de consultation: 07.06./2007).

<sup>20</sup> De cette problématique s'est occupé la Cour de Cassation dans son *Rapport 2005*. Dans la troisième partie, section « Innovation technologique et droit du travail », la cour affirme que « La machine et, surtout, l'électricité, qui a permis les ruptures technologiques majeures de la fin du vingtième siècle liées à l'informatique, ont, c'est un truisme banal, profondément altéré la relation de l'homme au travail en associant dans un inextricable ensemble la libération et l'asservissement au « code-barre » que devient l'homme). Le rapport est en ligne à l'adresse

(PSE/PSEM)<sup>21</sup>, la question des implants dans le corps humain et toutes les dérives éthiques sous-cutanées<sup>22</sup>, les problèmes de santé - notamment ceux qui sont liés aux effets thermiques - que poserait le spectre des ondes électromagnétiques utilisés par cette technologie, il nous convient de souligner que

- en dépit d'un regard spécifique, politique, ainsi que juridique, que l'UE veut donner à ce type technologique, les étiquettes RFID continuent à vivre la tension entre autonomie thématique et encadrement au sein du débat nanotechnologique. Pour tous, l'avis rendu du COMETS le 12.10.2006, portant sur les *Enjeux éthiques des nanosciences et nanotechnologies*, relève que « d'une certaine manière, les problèmes éthiques, légaux et sociaux soulevés par les nanosciences et nanotechnologies n'ont rien d'original. Par exemple, les atteintes à la liberté des individus, et à la vie privée, qui sont liées aux nanocapteurs-actionneurs et nanorobots sont déjà rendues possibles par les microtechnologies de l'information et de la communication ou les RFID » (p. 12)<sup>23</sup>. La tension dont nous parlons renvoie du reste à l'approche transdisciplinaire à

---

[http://www.courdecassation.fr/jurisprudence\\_publications\\_documentation\\_2/publications\\_cour\\_26/em\\_rapport\\_annuel\\_em\\_36/rapport\\_2005\\_582/](http://www.courdecassation.fr/jurisprudence_publications_documentation_2/publications_cour_26/em_rapport_annuel_em_36/rapport_2005_582/) (date de consultation : 07.07.2007).

<sup>21</sup> La question du bracelet électronique est inaugurée en France en 1989. Cf. BONNEMAISON G. Assemblée nationale, *Rapport 1989*. Du même auteur voir aussi *Face à la délinquance : prévention, répression, solidarité*, Rapport au Premier ministre - Commission des maires sur la sécurité, Doc. fr., 1983 (<http://lesrapports.ladocumentationfrancaise.fr/BRP/834037801/0000.pdf>; date de consultation 07.06.2007). Le débat est ouvert, notamment parce qu'une évaluation sur terrain doit encore être menée. Pour un panorama général cf. les documents du *National Council for Crime and Prevention* (<http://www.brottsforebygganderadet.se>). Cf. aussi ALBRECHT H.-J., *Electronic Monitoring in Europe. A Summary and Assessment of Recent Developments in the Legal Framework and Implementation of Electronic Monitoring*, Freiburg, 04.07.2005 ([http://www.mpicc.de/ww/de/pub/forschung/publikationen/onlinepub\\_print.htm#download](http://www.mpicc.de/ww/de/pub/forschung/publikationen/onlinepub_print.htm#download); date de consultation: 07.06.2007).

<sup>22</sup> Si en France une interdiction *stricto sensu* des implants sous-cutanés n'existe pas, en Italie M. Stefano RODOTÀ (en 2005 le Garant de l'Autorité italienne pour la protection des données personnelles) a introduit une prévision juridique spécifique en la matière. Cf. le document « *Smart (RFID) Tags* » : *Safeguards Applying to Their Use* (09.03.2005, doc. web n. 1109493 ; <http://www.garanteprivacy.it/garante/doc.jsp?ID=1121107>) a permis à. En appliquant la prévision de l'art. 154, 1<sup>er</sup> alinéa, lettre c) du Code le document précise : "Subcutaneous microchip implants in humans raise highly sensitive issues, which have already led other supervisory authorities in Europe to consider them unacceptable in terms of data protection. [...] In principle, subcutaneous microchip implants must be ruled out because they are in conflict with the dignity principle set forth in Section 2 of the Code, without prejudice to other legal provisions safeguarding bodily integrity and inviolability of personal dignity as also contained in the Charter of Fundamental Rights of the EU (Articles 1 and 3 thereof). Subject to data protection legislation and the provisions laid down herein, subcutaneous microchip implants may therefore be allowed only in exceptional cases further to documented, justified requirements concerning protection of individuals' health, by strictly complying with the proportionality principle (Section 11 of the Code) and fully respecting the data subjects' dignity (Section 2(1)). Data subjects should be in a position, as a rule, to have the microchips removed, at any time and free of charge, as well as to terminate the processing of data concerning them. [...] The Garante reserves the right hereby to order data controllers – also by means of generally applicable provisions - to subject RFID systems intended for subcutaneous implants to the Authority's prior checking pursuant to Section 17 of the Code, where said systems entail specific risks for data subjects' rights, fundamental freedoms, and dignity".

<sup>23</sup> Deux ans avant le rapport conjoint de la Royal Society et de la Royal Academy of Engineering *Nanoscience and nanotechnologies: opportunities and uncertainties* (9 juillet 2004) avait déjà fait le point sur les avantages et les désavantages de ces micro- et nanotechnologies : « nanotechnologies promise considerable advances in developing small and cheap sensing devices, enabling a range of features that will make smaller, longer-lasting sensors possible. [...] Such developments could be used to achieve greater safety, security and individualised healthcare, and could offer advantages to business [...]. However, the same devices might be used in ways that limit individual or group privacy by covert surveillance, by collecting and distributing personal information (such as health or genetic profiles) without adequate consent, and by concentrating information in the hands of those with the resources to develop and control such networks » (p. 54).

finalité holiste qu'utilise la convergence NBIC<sup>24</sup> [Bensaude-Vincent 07] qui aurait tendance à subtiliser les différences existant entre nature et artifice, matériel et immatériel en faveur d'un double propos : la réduction de la nature à la technique et la naturalisation du progrès technologique.

Au-delà de cette incertitude définitoire, l'évènement à la fois de la potentialisation et de la miniaturisation de ces objets ne cesse de poser tant des conflits de valeurs - liberté *versus* sécurité, liberté *versus* contrôle, liberté *versus* responsabilité, information *versus* anonymat, etc. - et de pouvoirs - technologique et législatif - que des lieux de redistribution de ceux-ci [Craipeau, Dubey, Guchet 04];

- dans un contexte d'interopérabilité des technologies au niveau communautaire et global des approches juridiques appropriées et convergents sont nécessaires. Le dialogue dernièrement mené parmi les organismes mondiaux de standardisation - nous pensons à l'ISO et l'IEC - soulève la question du manque de standardisation actuel [Banks, Pachano, Thompson, Hanny, 07]. Des standards en matière de production, de fonctionnement, de mise sur le marché des RFID devraient être discutés, approuvés et implémentés tenant en compte le critère d'acceptabilité culturelle, outre que les indispensables prémisses économiques. De plus, en matière d'harmonisation de l'usage de cette technologie la Déclaration de Montreux, approuvée par les Commissaires à la protection des données et à la vie privée lors de leur 27<sup>ème</sup> Conférence internationale (14-16.09.2005) a mis en évidence le besoin d'une reconnaissance universelle et partagée des principes de protection des données<sup>25</sup> ;
- sous un point de vue sociologique et anthropologique, la personne équipée dans une dimension de « sans contact » change progressivement sa configuration : une seule carte peut s'adresser à de multiples applications et lui permettre un accès sans limites dans un espace individué (cf. les cartes villes qu'on peut déjà trouver dans certaines villes des Pays-Bas). M. Maurizio FERRARIS parlerait dans ce cas-ci d'un « viandant sans papier » [Ferraris 07] pour lequel l'impératif sécuritaire n'est pas d'une importance primaire et les dimensions spatio-temporelles sont rebâties, les premières faisant place aux deuxièmes. « Le croisement de l'homme et de la machine » qui nous traverse et dont nous faisons expérience [Herrenschmidt 07] joue à la substitution du profil que l'informatique connaît traditionnellement - celui d'un usager tenant une position de consultant sur un poste client et étant en relation avec un poste serveur - avec un autre intégrant imperceptiblement l'objet à son sujet<sup>26</sup>. Pourtant l'intégration n'évite pas la permanence des enjeux traditionnelles de l'interconnexion, ce qui pourrait retracer la notion déclarative d'identité que nous connaissons en droit civil (« je suis... ») sur les mouvances réifiées et immatérielles de l'objet, des fichiers et des bases de données (la déclaration sur ton identité ne vaut que dans la mesure de ton individuation/authentification/identification);
- de façon symbolique, aux craintes traditionnelles liées à la figure dominante et unitaire du *Big brother* et aux utopies négatives orwelliennes [Orwell 49] se substitue le

---

<sup>24</sup> Cf. *Converging Technology for Improving Human Performance*, NSF-DOC Converging Technology Report, juin 2002 (<http://wttec.org/ConvergingTechnologies/>; date de consultation: 07.06.2007).

<sup>25</sup> Les Commissaires ont invité les différents sujets intéressés par la technologie à prendre des mesures spécifiques. La nouveauté réside pourtant dans le fait que la déclaration demande à l' « Organisation des Nations Unies à préparer un instrument juridique contraignant énonçant en détail le droit à la protection des données et à la vie privée en tant que droits de l'homme exécutoires ».

<sup>26</sup> Ce qui rappelle le débat sur la prothèse et le phénomène que les neurologues appellent 'proprioception'.

paradigme subtil et pulvérisé des *Little sisters*<sup>27</sup>. Pénétrant auprès de la personne et cohabitant constamment avec elle, ces technologies séduisantes de confort, de sécurité et de surveillance permettent la déconstruction de l'identité et sa reconstruction au sein d'une architecture modifiée de lieux et de relations, coordonnent la gestion des fluxes et des réseaux - inter- et intra-individuels, d'informations et de contacts -, reformulent les savoirs<sup>28</sup> selon une opérativité normalisante qui pourtant n'apparaît pas normalisatrice [Foucault 01].

### 3. Perspectives

Aucune réponse est complète au sujet de la technologie RFID. Cet état de l'art incertain - « le mauvais algorithme de chiffrement [...], le fait que le tag puisse répondre au lecteur sans l'accord de son possesseur » [Avoine 06] - invite les individus concernés à la vigilance informée, à la connaissance et à la pratique des droits déjà en vigueur, à une co-participation décisionnelle, car le droit est bien plus que « un outil technique de pure gestion sociale » et demande une interrogation collective et individuelle des valeurs en cause [Labrusse-Riou 89].

Au-delà des technologies de miniaturisation, les progrès techniques ont poussés le développement d'appareils d'analyse performants pour les biologistes : la puce à ADN a été mise au point au début des années 1990 et permet aujourd'hui d'effectuer des milliers d'analyses biologiques sur une surface de quelques millimètres carrés<sup>29</sup> ; le laboratoire sur puce à été élaboré pour la première fois à la fin du XX<sup>ème</sup> siècle et vise à réaliser les différentes étapes d'une analyse biologique depuis la préparation des échantillons jusqu'à ces résultats<sup>30</sup>.

Ces avancées technologiques sont ici à nous rappeler que la convergence disciplinaire - on le voit bien dans les domaines de l'électronique et de la génétique - représente une nouveauté absolue pour le droit, impliqué dans la reconnaissance des enjeux liant ces changements à la fois à *ce que* et à *ce qui* constitue la personne. Ne suffisant plus la référence timide que la loi n. 2004-800 du 6 août 2004 relative à la bioéthique a fait à l'art. L. 1418-1, 4 al. aux nanobiotechnologies - l'Agence de biomédecine a pour missions « de suivre, d'évaluer et, le cas échéant, de contrôler les activités médicales et biologiques, et notamment celles liées aux nanobiotechnologies, relevant de sa compétence et de veiller à la transparence de ces activités » -, il faudra bientôt que droit soit outillé afin de trouver des nouveaux repérages. Quelconque hypothèses serait pour l'instant imaginaire. Entre-temps le traditionnel principe de personnalité juridique (peut-être étendu jusqu'à la compréhension de son 'côté

<sup>27</sup> M. ALBERGANTI a récemment parlé de « small brothers » dans son ouvrage *La RFID et la démocratie*, Paris, 2007.

<sup>28</sup> G. O. LONGO affirme à ce propos que « notre civilisation a vu un développement selon une double destitution, celle du corps et celle du génie [...] Par le biais de la raison, de la rationalité computiste, l'homme cherche à rebâtir la réalité, ainsi substituant aux monde donnée [...] un monde mesuré et dominable [...] en mesure de lui permettre la survivance » (LONGO G. O., « Riduzionismo informazionale e postumano », in *Kainós. Rivista online di critica filosofica*, 6/2006, n.t.). L'article est chargeable à l'adresse <http://www.kainos.it/numero6/ricerche/ricerche-longo-postumano.html> (date de consultation: 07.07.2007). Ce contenu reprend en gros celui de l'ouvrage du même auteur *Homo technologicus*, Milan, 2001.

<sup>29</sup> L'usage de macromolécules d'ADN, capables de quitter leur chaîne d'origine, de se déplacer et de s'attacher à d'autres chaînes, en fin de revenir à la structure de base permettait une grande flexibilité d'action et une meilleure performance du produit. En 2004 un mini-robot bipède avait été crée utilisant l'ADN. En janvier 2007 un nanobras a été mis au point par la même équipe (Nadrian Seeman et Baoquan Ding, de l'université de New York).

<sup>30</sup> Dans ce cadre le CEA de Grenoble a mis au point un labopuce baptisée Biochiplab. Ceci devrait en futur permettre aux chercheurs une étude de très petits échantillons.

électronique'), ceux de sauvegarde de la dignité humaine et de l'intégrité corporelle, le plus récent principe de précaution pourront faciliter le processus.

## Bibliographie

- Avoine, G. : « RFID et sécurité font-elles bon ménage ? », in *Actes du Symposium sur la Sécurité des Technologies de l'Information et des Communications (SSTIC)*, consultation à partir de l'adresse [http://actes.sstic.org/SSTIC06/RFID\\_et\\_securite/](http://actes.sstic.org/SSTIC06/RFID_et_securite/) Date de consultation : 06.06.2007).
- Banks, J., Pachano, M., Thompson, L., Hanny, D.: *RFID in the United States*, RFID Applied, 10 avril 2007, pp. 445-456.
- Bensaude-Vincent, B.: *Se libérer de la matière ? Fantômes autour des nouvelles technologies*, Paris, 2004.
- Carbonnier, J. : *Droit civil. Les personnes*, Paris, 2000, vol. 4, p. 243 ss.
- Craipeau, S., Dubey, G., Guchet X. : *Rapport sur les usages et représentations de la biométrie*, février 2004.
- Dupuy J. P.: *Pour une catastrophe éclairée*, Paris, 2002.
- Dupuy ; J-P, Roure, F. : *Les nanotechnologies. Ethique et la prospective industrielle des nanotechnologies*, Conseil général des Mines, avril 2005.
- Edelman, B. : « La personne et ses attributs », in *La personne en danger*, Paris, 1999, p. 111.
- Edelman, B. : « Sujet de droit et technoscience », in *La personne en danger*, Paris, 1999, pp. 397-416.
- Ferraris, M. : *Sans papier. Ontologia dell'attualità*, 2007, Roma, p. 131.
- Foucault, M. : *Dits et écrits*, vol. 1 et 2, Paris, 2001.
- GEE, *Aspects éthiques ses implants TIC dans le corps humain*, Bruxelles, doc. n. 20, 16 mars 2005.
- Hermitte, M.-A. : « Le Corps hors du Commerce, hors du Marché », in *Archives de philosophie du droit*, Paris, 1988, p. 120.
- Herrenschmidt, C. : *Les trois écritures*, Paris, 2007.
- Josserand, L. : *La personne humaine dans le commerce juridique*, D, 1932, 1.
- Labrusse-Riou, C : « Les implications juridiques de la génétique » in *Revue du droit public et de la science politique en France et à l'étranger*, 1989, p.1369.
- Labrusse-Riou, C. : « Le corps à l'épreuve des biotechnologies. Perspectives juridiques », in *Cahier de l'École des sciences philosophiques et religieuses*, n.18, Saint-Louis (Bruxelles), 1995, p.38.
- Labrusse-Riou, C. :« Le corps hors du droit », in *Les urgences du droit*, cité par M. Fabre-Magnan, préface à l'ouvrage de Labrusse-Riou, C. : *Ecrits de bioéthique*, Paris, 2007, p. 8.
- Longo, G. O. : *Homo technologicus*, Milano, 2001.
- Orwell G.: *1984*, New York, 1949.
- Pedrot, P. (dir.) : *Traçabilité et responsabilité*, Paris, 2003, Intr., p. X.
- Rodotà, S. : *La vita e le regole. Tra diritto e non diritto*, Roma-Bari, 2006.
- Strickler, Y. : *Les biens*, Paris, 2006, p. 121.