

Rapport général introductif

Yves Poulet

Professeur, Directeur du CRID, Facultés universitaires de Namur

Antoinette Rouvroy

Chercheur au CRID

1. Le titre de la conférence confirme d'emblée la complémentarité de l'éthique et des droits de l'Homme. Aux fondements, et à l'horizon des droits de l'Homme, se trouvent des valeurs éthiques. L'approfondissement de ces dernières dans un contexte changeant éclaire la portée à donner à la proclamation des droits de l'Homme. En retour, le respect effectif des valeurs éthiques présuppose l'affirmation et la mise en oeuvre des droits de l'Homme.

2. Le fait que l'UNESCO et la Commission française pour l'UNESCO aient choisi le Conseil de l'Europe comme lieu et partenaire pour cette conférence régionale est une seconde confirmation de cette complémentarité. L'UNESCO, défenseur des principes éthiques, s'allie avec le Conseil de l'Europe qui porte si haut à la fois la cause des droits de l'Homme et celle de l'Etat de droit. C'est dans ce double héritage que nous puiserons les bases de notre réflexion,

3. La seconde partie du titre de la conférence nous amène à nous intéresser ensuite aux évolutions majeures de notre société de l'information. Il s'agit de comprendre en quoi cette société réclame une attention renouvelée aux valeurs éthiques fondatrices des droits de l'Homme.

4. L'une des caractéristiques de la société de l'information ou plutôt de l'infrastructure qui prétend la porter, à savoir le réseau des réseaux, l'Internet, est son caractère global ou mondial. Internet est, qu'on le veuille ou non, le lieu global où s'expriment mais aussi et de plus en plus, où s'affrontent de multiples visions du monde jusque là maintenues séparées derrière des frontières physiques.

La question qu'il importera donc de se poser dans le chapitre II est celle de savoir si ces visions, nonobstant les divergences culturelles liées à l'identité des communautés qui les soutiennent, peuvent s'accorder sur quelques valeurs communes leur permettant d'entrer en dialogue afin de garantir leur coexistence pacifique. Si tel n'était pas le cas, il y aurait tout lieu de craindre qu'Internet ne devienne une tour de Babel où la peur et la haine du discours de l'autre aboutiraient à la perte de cette chance unique et inédite d'un enrichissement culturel, intellectuel, politique et humain de la société globale.

Ces valeurs éthiques communes, nous croyons les déceler en filigrane des documents internationaux promus par l'UNESCO et acceptés universellement, en matière de bioéthique : dignité et autonomie de la personne humaine; solidarité entre les hommes et les peuples et justice sociale ; impératif de bienfaisance et de prévention des effets dommageables des technologies.

Ces mêmes valeurs trouvent dans les droits de l'Homme leur traduction et leur prolongement. En même temps, la signification des droits qui consacrent ces valeurs doit être relue en

fonction des nouveaux risques d'atteintes à ces valeurs dans le contexte de la société de l'information.

Ainsi, dignité et autonomie de la personne ont traditionnellement trouvé écho dans le droit à la protection de la vie privée, entendue au sens le plus large, y compris dans sa dimension « protection des données ». Les valeurs de solidarité et de justice sociales ont suscité l'émergence de droits tels que le droit d'accès universel et le droit à la diversité des expressions culturelles. Enfin, les impératifs de « bienfaisance » et de « non-maleficence » ont trouvé récemment des prolongements juridiques.

5. Ce dernier point nous amènera à une réflexion finale. Au-delà de l'éthique et des Droits de l'Homme et afin d'assurer l'effectivité de leur respect, sans doute faut-il affirmer la nécessité que la conception et le développement des technologies nouvelles soient accompagnés de procédures de décision démocratiques et fondés sur les valeurs (democratic and value sensitive design of ICT). Dans la mesure en effet où ces technologies nouvelles façonnent, d'une manière de plus en plus déterminante, l'architecture informationnelle de l'espace public mondial, leur nature est éminemment politique.

I. L'UNESCO et le Conseil de l'Europe : deux approches complémentaires pour parler de la société de l'information

6. L'apport des travaux de l'UNESCO à la problématique des valeurs éthiques et des droits de l'Homme aux présents débats est substantiel et crucial. Sans doute, on citera la Recommandation de 2003 sur l'accès universel et la promotion du multilinguisme¹, mais on pointera également deux textes majeurs : le premier est la *Convention sur la diversité des expressions culturelles* de 2005² qui plaide clairement pour la reconnaissance, la protection et la promotion des nombreuses identités culturelles, ... y compris dans le cyberspace. Le second est la Déclaration universelle sur la Bioéthique et les droits de l'Homme de 2005³. Nous nous interrogerons sur l'intérêt de reprendre, à propos de la société de l'information, les principes éthiques adoptés internationalement en matière de bioéthique.

7. Si l'UNESCO apporte à notre réflexion la dimension éthique qui convient et si l'UNESCO met en exergue, parmi les valeurs éthiques, le respect de l'identité culturelle de chaque communauté, l'héritage du Conseil de l'Europe ajoute d'autres dimensions à notre réflexion. La Convention de 1950 sur les droits de l'Homme met en relief le besoin de traduire, sous forme de droits et de libertés fondamentales, les valeurs éthiques. Parmi ces droits et libertés reconnus, deux sont particulièrement pertinents pour notre propos : le droit à la protection de la vie privée et le droit au respect de la liberté d'expression, consacrés respectivement par les articles 8 et 10 de la Convention de 1950⁴.

Au-delà de ces deux articles piliers, on citera des instruments plus spécifiquement centrés sur les technologies de l'information et de la communication : la Convention n° 108 de 1981 en matière de protection des données⁵ d'une part, et la Recommandation sur la libre expression dans la société de l'information⁶. Ces textes témoignent :

- du fait que les droits de l'Homme sont fondés sur les valeurs éthiques et doivent être interprétés à partir de celles-ci. Dans cette interprétation, on tient compte de l'évolution du contexte sociétal dans lequel ces valeurs ont à s'exprimer⁷ ;
- du fait que l'Etat se voit reconnaître un rôle important pour garantir et promouvoir ces droits et libertés⁸ ;

- de l'effet horizontal des droits de l'Homme, qui implique que les particuliers ont également le devoir mutuel de respecter les droits et libertés fondamentaux reconnus à chacun d'eux⁹.

Il importe donc de comprendre la façon dont la société de l'information peut affecter les valeurs éthiques et les droits de l'Homme ou libertés affirmés par les institutions qui aujourd'hui organisent notre rencontre.

II. La société de l'information : tendances majeures¹⁰

A. L'imprévisibilité des développements de la technologie

8. L'imprévisibilité des développements industriels et applications potentielles des nouvelles technologies de l'information et de la communication constitue en soi un premier défi inhérent à la 'gouvernance' de la société de l'information. Ainsi, les cookies ont été créés pour assurer la continuité d'une session ouverte par un terminal avec un site web. Les applications des cookies, en particulier dans le domaine du *one to one marketing*, couplés avec des hyperliens invisibles, attestent de la possibilité d'utiliser une technologie dans un tout autre objectif que celui prévu initialement. La même remarque vaut pour les technologies RFID¹¹ au départ imaginées pour remplacer la technologie du code barre dans des applications logistiques et aujourd'hui omniprésentes dans les objets, les vêtements, les passeports, voire le corps humain pour des raisons de sécurité, de surveillance, de marketing ou à des fins de suivi et de surveillance médicale¹².

Cette première constatation nous conduit à exprimer deux mises en garde qui concernent respectivement les politiques en matière de propriété intellectuelle, et la nécessité d'une plus grande coordination entre l'UNESCO et le Conseil de l'Europe d'une part, et les institutions de l'Union européenne d'autre part. En matière de propriété intellectuelle, alors que la tendance actuelle est à la multiplication des brevets et autres droits d'exploitation exclusifs dans tous les domaines technologiques, la « totipotence » des nouvelles technologies de l'information, de la communication et de la réseautique d'une part, et la très forte probabilité d'une convergence croissante entre TICs, biotechnologies et neurosciences, nécessite que l'on réévalue à nouveaux frais l'incidence des brevets d'invention sur l'innovation technologique. Au lieu de se hâter par les droits de propriété intellectuelle (brevet, droit d'auteur) à consacrer l'appropriation privative d'une technologie, le droit ne doit-il pas veiller à ce que cette appropriation n'ait pas sur le développement des applications de ces technologies un impact négatif ? Outre cela, il apparaît également urgent de nous demander si le respect des valeurs éthiques et des droits de l'Homme ne devrait pas s'imposer comme condition additionnelle à la brevetabilité des inventions dans le domaine des TICs, de la même manière que cette condition a été imposée par le Conseil et le Parlement de l'Union européenne dans le domaine des inventions biotechnologiques.¹³ En tout état de cause, l'imprévisibilité des applications TICs rend, plus encore que jamais, indispensable le dialogue non seulement entre l'UNESCO et le Conseil de l'Europe, mais également entre ces deux institutions et les institutions de l'Union européenne, dans la mesure notamment où les directives européennes en matière de brevetabilité, mais aussi les programmes de financement européens en matière de recherche et de développement ont un impact indéniable sur l'orientation des développements de la société de l'information. L'évolution de la société de l'information invite donc à repenser les modalités d'interactions et de coopération institutionnelles sous peine d'ajouter au défi induit par l'imprévisibilité des applications technologiques, celui de l'imprévisibilité du

développement normatif aussi dommageable pour l'innovation technologique que pour le respect des valeurs éthiques et des droits de l'Homme.

B. Les grandes évolutions des systèmes d'information

9. Le développement des technologies de l'information peut se laisser décrire, chronologiquement, comme la succession de trois évolutions : la première, connue sous le nom de « loi de Moore », consiste en l'accroissement continu des capacités des ordinateurs, des terminaux et des infrastructures de communication ; la deuxième coïncide avec la « révolution de l'Internet » ; enfin, la troisième consiste en une révolution plus profonde encore, celle de l' « intelligence ambiante » qui met la technologie et le réseau au cœur du réel : de nos objets, des lieux et des corps.

a) La loi de Moore¹⁴

10. La loi de Moore s'exprime comme suit. Tous les 18 mois, la capacité de stockage des ordinateurs est multipliée par deux pour le même prix, ce qui signifie la multiplication par 1000 en 15 ans. Les capacités de transmission de nos réseaux augmentent dans des proportions semblables. Cette augmentation des capacités de stockage, de traitement et de transmission explique qu'en quelques secondes, Google puisse faire droit à votre demande, scannant plus d'un milliard de sites dans le monde. Cette augmentation explique que désormais enregistrer tous les faits et gestes de la vie d'un individu n'est plus chose impossible avec un ordinateur personnel.¹⁵ L'expérience, baptisée "LifeLog", de l'enregistrement de la totalité des événements, expériences et interactions d'une personne avec le monde qui l'entoure est d'ailleurs en cours dans le cadre d'un projet de l'Information Processing Technology Office (IPTO), une agence de la Defense Advanced Research Projects Agency américaine.

b) L'évolution de l'Internet

11. La révolution de l'Internet à laquelle nous continuons d'assister présente des dimensions diverses. Il est de coutume d'insister sur la globalisation des échanges qui me permet, sans bouger de l'endroit où je me trouve, d'atteindre les quatre coins du monde. L'on parle également, invoquant les modèles de quatrième génération des télévisions interactives, de la convergence de tous les réseaux, là où nos activités de communication étaient jusque là séparées, véhiculées par des infrastructures différentes. Notre propos ne s'arrête pas là. Afin de mieux inter-opérer, de dialoguer entre eux, de pouvoir comprendre les messages transmis, le web est devenu sémantique¹⁶, ce qui veut dire que l'ordinateur lui-même crée des métadonnées à partir de données qu'il stocke ou envoie de manière à ce que, plus facilement, les personnes, voire les ordinateurs, puissent à distance accéder et analyser leur contenu. Les services d'analyse automatique des courriers e-mail sont un bel exemple de cette dimension nouvelle. Nous ne saurions trop insister sur le fait que cette création de métadonnées, qui permet de découvrir l'information à travers le filtre de mots-clefs et de la conceptualisation inhérente au web sémantique, n'est plus nécessairement ni volontaire ni consciente dans le chef de celui que l'on nomme l' « utilisateur », mais bien plutôt le résultat d'opérations automatiques réalisées par l'ordinateur.

12. Une autre évolution remarquable de l'Internet résulte de la disponibilité et de l'utilisation de méthodes d'identification et d'authentification des acteurs/utilisateurs du net qui leur permet à la fois de se faire connaître ou reconnaître lorsque cette « identification »

conditionne l'accès à une ressource, un service ou une information et, au-delà, de pouvoir les identifier de manière sûre lorsqu'il s'agit de « recomposer » de l'information à leur propos, à partir d'éléments d'information dispersés dans des bases de données distribuées dans le réseau et ce, sans limites de frontières. On note que ces « digital identities »¹⁷ constituent alors des métadonnées. Enfin, soulignons que ces identités digitales peuvent, avec les technologies de la biométrie (l'iris, l'empreinte des doigts, la voix), « s'incarner » dans des caractéristiques physiques et corporelles, réduites à leurs représentations en données.

c) L'intelligence ambiante : où le virtuel rejoint le réel¹⁸

13. Sans doute faut-il d'abord évoquer les nombreux services de localisation spatiale qui offrent une aide au destinataire spécifique au lieu où il se trouve (services de navigation, mais également services relatifs aux caractéristiques de l'environnement).

Les réseaux d'intelligence ambiante ont pour objet de mettre la personne et son environnement directement en interaction. L'intelligence que permettent les TIC et l'accès au cyberspace est dorénavant répartie dans les choses, les lieux, voire nos corps, dans lesquels la technologie se fond pour devenir une seconde nature.¹⁹ Ces technologies de l'intelligence ambiante doivent leur développement à l'extrême miniaturisation des terminaux (cf. les RFID, terminaux de la taille d'un grain de riz et les nanotechnologies²⁰ encore dans l'enfance de la recherche et leur connexion via des capteurs et l'Internet à des systèmes d'information). Les applications sont multiples qui permettent par exemple de suivre le parcours d'un consommateur dans un supermarché et, grâce au « dialogue » entre la puce du consommateur et celles des produits, de comptabiliser automatiquement les achats effectués. Elles peuvent aussi permettre de lire, à distance, des passeports, « faire commander » automatiquement, par un « frigo intelligent » la bière manquante, ou encore faire en sorte qu'un poste de télévision repère automatiquement votre présence et envoie l'image du programme adéquat automatiquement vers l'écran de l'ordinateur personnel de votre bureau. Les applications sont infinies. Elles permettent de caractériser l'intelligence ambiante comme suit.

On parle d'« Ubiquitous computing » : une technologie de l'ubiquité dans la mesure où les terminaux peuvent être placés partout et dès lors enregistrer les faits les plus anodins de notre vie quotidienne, nos déplacements, nos hésitations, notre consommation domestique. Cette technologie est ensuite une technologie largement invisible (« calm technology ») dans un double sens : elle fonctionne de manière opaque, invisible (nous ne connaissons pas le circuit d'information sous-tendant le fonctionnement de la puce : qui la lit ? Quand ? Quelles informations ? Pour qui ?), mais également elle apparaît comme le prolongement naturel même de notre action (la porte s'ouvre et l'ordinateur s'allume) mettant les choses à notre service. Enfin, cette technologie est dite « apprenante » (« learning technology »). Ses applications ont souvent en effet pour caractéristique d'adapter leur fonctionnement aux données obtenues de par leur utilisation. Ainsi, dans le cas du grand magasin, le système tiendra compte de nos achats précédents pour progressivement mieux nous profiler et nous adresser la publicité appropriée.

14. Ainsi, les technologies d'intelligence ambiante ont pour conséquence d'associer **le virtuel et le réel**. Au sein des réseaux créés par le dialogue entre les choses entre elles ou avec l'homme, c'est l'espace réel qui se trouve investi par les TIC.

Au sein de ces réseaux, l'homme, *in fine*, peut devenir une « chose » elle-même insérée dans une relation avec d'autres choses qui réagissent à la présence de cette chose.

On évoquera enfin les questions liées aux applications dites « médicales »²¹ des RFID implantés dans le corps humain qui permettent à distance de connaître le fonctionnement de celui-ci, voire de « corriger » ce fonctionnement, par exemple remédier à un état de stress ou stimuler la mémoire.

C. Les logiques « absolues » qui soutiennent le développement des technologies

15. Cinquante pour cent des habitués des « Baya Club », une société de gestion de dancings et maisons de jeux situés en Hollande et Espagne, ont accepté de se voir implanter une puce RFID dans le corps²². Aux journalistes qui s'inquiétaient de leur acceptation, ceux-ci répondent qu'une telle puce facilite grandement leur passage aux entrées du casino où la lecture de la puce permet de reconnaître comme « bons » clients et, par ailleurs, leur permet de ne pas courir le risque de se voir voler leur portefeuille, inutile dans la mesure où les consommations sont directement débitées de leur carte de crédit.

Cet exemple – et on pourrait les multiplier – illustre combien les logiques sécuritaires et d'efficacité économique (gain de temps, voire d'argent) expliquent le succès des applications des technologies de l'information et de la communication. On connaît les arguments utilisés à l'appui de la mise au point de la puce RFID que le gouvernement américain entendait implanter dans le corps de tout citoyen américain pour qu'en cas d'accident et d'inconscience de ce dernier, on puisse l'identifier et connaître les données médicales d'urgence.

Ainsi, la sécurité publique mais également privée des organisations et des citoyens exige toujours davantage de systèmes de contrôle, de surveillance et d'alerte. La rentabilité économique, au sens le plus large, l'efficacité tout court, viennent comme une justification complémentaire où se rejoignent les préoccupations des administrations et des organisations, d'une part, et les intérêts des consommateurs et des citoyens, intérêts soigneusement mis en évidence par les administrations ou organisations.

D. La privatisation du cyberspace

16. Sous ce point, on souligne bien évidemment le fait que les normes applicables dans le cyberspace et le fonctionnement du réseau (adresses IP, protocoles web, ...) échappent en grande partie aux autorités publiques qu'elles soient nationales, régionales ou internationales²³. La gouvernance de l'Internet est privée²⁴. Elle est l'œuvre d'abord d'organisations privées internationales et en tout cas elle résulte de la discussion de sociétés privées plus que d'arbitrages interétatiques.

La privatisation du cyberspace prend une autre signification lorsqu'on doit bien constater que l'accès à ce cyberspace, tant pour les destinataires que ceux qui veulent y mettre du contenu, se trouve conditionné au respect des exigences imposées par certains acteurs, les fournisseurs d'accès, les portails, les moteurs de recherche qui peuvent orienter notre recherche de l'information, notre navigation et la soumettre à l'acceptation par nous de règles du jeu, telles la publicité, l'identification, etc. C'est souvent eux aussi qui apposeront des filtres, des limites, voire des procédures de censures et s'auto-constitueront ainsi, tacitement, en régulateurs de l'espace public qu'est Internet.

Toujours dans le même sens, on connaît la contestation que soulèvent certains « Digital Rights Management Systems²⁵ » lorsque la technique, bien au-delà des principes et de la

logique des droits de propriété, clôture l'œuvre et en restreint excessivement l'accès, au détriment de l'exercice, par d'autres, de leurs libertés fondamentales²⁶.

E. La portée globale d'actions ou de décisions d'acteurs locaux

17. Parmi ces acteurs, on épinglera bien évidemment les entreprises qui offrent des services grâce à ces technologies. La façon dont leurs produits ou services sont construits peut avoir des répercussions sur l'ensemble de la planète lorsque la puissance économique que ces entreprises détiennent est telle qu'elle leur permet de décider des conditions d'accès à l'information ou de publication de contenus d'une partie de la population mondiale. Il faut bien se rendre compte notamment que l'Internet décuple la puissance de certaines entreprises de presse.

18. Mais l'Internet décuple également la puissance de l'individu lui-même qui, de manière ciblée ou diffuse, consciemment ou inconsciemment, peut, par un simple message posté sur le net, une simple information sur son blog, porter atteinte à la réputation d'autrui, transmettre un virus, envoyer ou consommer des contenus pédo-pornographiques et de ce fait encourager la traite des êtres humains, autant d'actes faciles à poser localement qui peuvent avoir des répercussions dommageables jusqu'à l'autre bout de la planète. Internet confère donc à nos actes, même individuels, et sans aucun effort particulier de notre part, une portée « globale » qui n'est pas sans reposer la question de la responsabilité individuelle et collective. Il nous paraît peut-être prometteur, à cet égard, de penser en terme d'écosystème informationnel, de la même façon que les défis actuels posés par la dégradation de l'environnement naturel nous ont induit à penser nos responsabilités individuelles en termes plus globaux. Sans doute, une autre dimension des relations humaines, de plus en plus cernée par les technologies de l'information et de la communication, celle de l'espace, inviterait donc à s'inspirer des principes d'une éthique de l'environnement. Les principes du développement durable et surtout ceux du risque partagé et de précaution mis en évidence dans cet autre domaine mais qui n'ont pas encore fait l'objet du même consensus que celui qui s'est dégagé dans le domaine de la bioéthique pourraient également nous être utiles.

Ils seront évoqués dans la suite de l'exposé.

III. Société de l'information et enjeux éthiques

A. Où il est question de bioéthique

19. Les organisateurs de ce colloque ont placé en tête de leurs préoccupations pour le débat d'aujourd'hui la question des valeurs éthiques.²⁷ A l'heure où chacun se réfugie derrière ses droits subjectifs ou les proclame, il est intéressant de rappeler que le droit, s'il n'est pas la pure traduction de principes éthiques, doit cependant ne point les heurter et, si possible, en favoriser l'accomplissement.

La difficulté de l'exercice, dans une société globale qui se doit d'être respectueuse des valeurs et identités culturelles qui s'y côtoient, voire s'y affrontent, est de trouver des valeurs communes de référence, acceptées universellement.

20. Précisément, le champ de la bioéthique nous est apparu comme pouvant fournir certaines indications utiles dans la recherche de cette base commune.²⁸ Par sa déclaration de 2005 déjà

évoquée²⁹, l'UNESCO a pu dégager un accord international sur des valeurs éthiques communes³⁰ dont nous constaterons toute la résonance dans le domaine de la société de l'information. Ce consensus obtenu est d'autant plus respectable et respecté qu'il a été atteint au terme d'une approche non point dogmatique mais, au contraire, fondée sur une analyse de différents cas et en tenant compte des évolutions technologiques dans le domaine de la biomédecine.

Le rapprochement entre bioéthique et éthique de la société de l'information que nous suggérons n'est pas seulement d'opportunité. Il se justifie également par le fait que, dans les deux domaines, il est question de l'identité humaine et de la position des individus face aux technologies.

On ajoute que les deux domaines se rejoignent de fait depuis assez longtemps, depuis, plus précisément, le « tournant linguistique » emprunté par la biologie moléculaire dans les années 1970 et l'émergence de la cybernétique, mettant au centre des processus biologiques eux-mêmes la notion d' « information »³¹.

B. De quelles valeurs éthiques parlons-nous ?

21. Au risque de caricaturer un peu leur compréhension dans l'ordre de la bioéthique, nous proposons de retenir trois types de valeurs éthiques qui s'imposent **à la fois à la recherche et aux développements des technologies tant du vivant que de l'information et de la communication, et à l'utilisation des applications découlant de la recherche**. Il s'agit des valeurs de **dignité humaine et de l'autonomie**. Sans doute, la dimension éminemment collective des technologies de l'information et de la communication nous amènera à nous interroger sur l'intérêt d'affirmer non seulement la valeur de l'autonomie individuelle mais également celle des communautés.

La dignité humaine³² renvoie, selon l'approche kantienne, à la reconnaissance inconditionnelle, inaliénable et universelle de tout être humain vivant, quel que soit le degré d'autonomie dont il est de fait capable, comme une fin en soi, et jamais comme un moyen.

L'autonomie de l'individu³³ ou son autodétermination consiste en son aptitude à déterminer son propre bien, sa propre conception de la vie bonne et, dès lors, à pouvoir contribuer pleinement à une délibération collective. Il ne s'agit point d'une liberté robinsonienne³⁴ où la liberté serait sans limites mais, au contraire, de la liberté d'une personne « située » à l'intérieur d'une ou plusieurs collectivités et qui doit pouvoir apporter à celles-ci la pleine valeur de son apport original. En ce sens, l'autonomie est un bien collectif ; elle constitue une condition de l'apport de chacun à la démocratie délibérative.

L'autonomie collective d'une communauté culturelle s'entend également de la possibilité pour celle-ci de façonner, de développer, de vivre et d'exprimer son identité et d'enrichir ainsi le patrimoine culturel de l'humanité³⁵.

22. La solidarité et la justice sociale, qui composent ensemble le second impératif éthique, celui de la justice, se déclinent comme suit. La **solidarité**, première valeur de ce second type peut être approchée comme suit. L'on présente souvent la valeur de la solidarité comme fondée sur la conscience que nous partageons la même vulnérabilité mais de manière plus ou moins accusée. Cette reconnaissance du poids différencié de cette vulnérabilité suivant que l'on est riche ou pauvre, vivant dans telle ou telle région, ayant un accès plus ou moins facile

à l'éducation, à la culture et à l'information fonde notre responsabilité morale d'être solidaires les uns envers les autres. Le devoir de solidarité se fonde ainsi sur la reconnaissance du caractère moralement arbitraire des inégalités de vulnérabilité, inégalités évidentes que nous constatons autour de nous, davantage encore que sur le partage d'une vulnérabilité commune, toute théorique. C'est la reconnaissance de degrés de vulnérabilité différents dont l'on reconnaît qu'ils ne sont pas « mérités », c'est-à-dire qu'ils sont dus, davantage qu'au mérite individuel, à l'effort etc., à la chance ou à la malchance – à commencer par celle d'être né dans telle ou telle région du monde, avec tel ou tel handicap. Nous connaissons de plus en plus précisément les inégalités dans la répartition des vulnérabilités, mais nous savons aussi, et c'est en cela que la solidarité est bien une exigence de justice, qu'il est injuste que les « malchanceux » aient à supporter seuls le poids de leur malheur, et que les « bien nantis » n'aient pas à partager ce dont ils jouissent par la chance d'être bien nés.

23. C'est donc bien le savoir de notre inégale vulnérabilité qui fonde l'obligation de solidarité et non pas l'intuition, bien aveugle aux inégalités de fait, d'une commune vulnérabilité. Rien n'est moins commun, dans un monde divisé, que la vulnérabilité. Toujours est-il que le devoir de solidarité impose de reconnaître que les choix, qui nous regardent au premier titre, ont ou peuvent avoir un impact sur la liberté de choix des autres. ***La solidarité, c'est-à-dire la prise en compte des effets de nos décisions propres sur autrui constitue le prérequis d'une participation éthique à la société de l'information. (Je mettrais plutôt cette dernière remarque au titre du principe de « bénéficienne » et de « non maléficienne »).***

Le principe de la justice sociale est un principe de mise en œuvre collective du devoir de solidarité. Il s'agit de l'exigence morale de réduction des inégalités d'accès et de participation dans la société (en l'occurrence, la société de l'information), ainsi, pour les personnes âgées, les pauvres, les handicapés, les populations du Sud, et de veiller à une représentation loyale et équitable des différents intérêts sociaux, culturels, économiques dans la gouvernance de la société. Il est clair que la référence à cet impératif de justice aura également pour conséquence d'éviter que l'usage ou certains usages des technologies soient réservés à une population déterminée et ce, de manière discriminante.

24. Enfin, l'objet technologique mis à la disposition de l'intervention sur le vivant ou, dans le cas qui nous occupe, utilisant le traitement de l'information ou sa communication doit, dans son développement, être guidé par deux principes : celui de la « bienfaisance », c'est-à-dire de l'apport bénéfique et, à l'inverse, celui de la « non-maleficence »³⁶, c'est-à-dire le rejet d'une technologie dont la structure, le « design » porterait en lui-même des risques négatifs pour l'individu et/ou pour la société dans son ensemble.

Ainsi, le premier principe conduit à des choix technologiques qui chercheront à maximiser l'apport bénéfique de ces technologies sur la population. A l'inverse, le second principe appelle au rejet de toute technologie dont le fonctionnement ou le design pourraient avoir un impact négatif sur la sécurité ou le bien-être des individus ou des collectivités. Encore convient-il – et c'est en cela que les principes éthiques de respect de l'autonomie, de justice et de bienfaisance entrent en interaction – que ce « bien », que l'on cherche à faire advenir au moyen des technologies, soit défini en tenant compte de la diversité des points de vue et des intérêts en jeux, ce qui implique bien évidemment la mise en œuvre de processus décisionnels de nature à garantir cela.

L'existence de ces deux principes – bienfaisance et non-maleficence - suppose le respect d'un troisième principe : le principe de précaution³⁷ qui veut que lors de sa mise au point, chaque

technologie fasse l'objet d'une évaluation relative aux risques sociétaux, sanitaires et écologiques potentiellement induits par ladite technologie et que l'autorité publique puisse dès lors intervenir, le cas échéant, pour procéder à cette évaluation. L'instauration d'organismes interdisciplinaires de « veille technologique » pourrait être intéressante à cet égard.

C. Valeurs éthiques et technologies de l'information et de la communication (TIC)

1. Autonomie et TICs

25. A force d'insister sur les menaces induites par les nouvelles TICs, l'on en oublierait presque de souligner ce qui pourtant paraît indéniable : que l'utilisation des technologies de l'information peut aussi, bien évidemment, fournir des ressources inédites à l'individu pour développer son autonomie. Il est certain que l'outil, en particulier Internet, favorise au plus haut point la possibilité pour chacun de découvrir et discuter la pensée d'autrui, de collecter l'information nécessaire à son jugement et de participer à la formation de l'opinion publique. Au-delà, on note que l'utilisation de l'outil lui permet d'échapper aux contraintes de lieux et de temps et, plus encore, aux entraves culturelles et sociales que peuvent lui imposer son milieu. Enfin, l'internaute peut, sous couvert d'un pseudonyme, expérimenter plusieurs manières d'être lui-même, jouer tous les rôles et épuiser tous les possibles.

26. A cette vision très positive, s'opposent des images plus pessimistes : celle de l'internaute faisant face au « *Big Brother* »³⁸ du roman d'Orwell, personnage qui amasse l'information et peut tout décider face à un internaute de plus en plus transparent, celle, inspirée du Procès de Kafka³⁹, d'un sujet affrontant une machine dont le fonctionnement totalement opaque et sans logique l'empêche d'anticiper les conséquences des actes qu'il pose.

Ainsi, on évoque les dangers nés :

- du déséquilibre des pouvoirs respectifs⁴⁰ des responsables des traitements, d'une part, et de la personne concernée, d'autre part. Ce déséquilibre peut conduire à toutes les discriminations ;
- de la « décontextualisation »⁴¹ : les données qui circulent sur la toile ont été « émises » par les personnes concernées pour une finalité précise ou dans un contexte particulier. Les croisements de données de toute sorte et la possibilité d'interroger les moteurs de recherche à partir de n'importe quel mot-clé engendrent la crainte que nous soyons jugés « hors contexte » ;
- de l'opacité⁴² du fonctionnement tant des **terminaux** (les cookies, les RFID) que des **infrastructures** (voir les « agents distribués » localisés tout au long de systèmes d'information comme ceux dits d'intelligence ambiante). Cette opacité entraîne la crainte de traitements non sollicités, non voulus et la volonté dès lors de se conformer à un comportement qui est celui que nous pensons être attendu en ces nouveaux lieux invisibles de surveillance ;
- du **réductionnisme**⁴³ : de plus en plus, les données collectées à propos des événements même les plus insignifiants de notre vie se multiplient et les systèmes d'information nous analysent à travers ces données qui réduisent les choix et vies humains, de même que nos personnalités, à des « profils » créés en fonction de conceptions en vue de finalités définies par ceux qui utilisent ces données, voire directement par le dispositif technologique⁴⁴. Dans les systèmes d'intelligence ambiante où l'homme est mis en réseau avec un ensemble d'objets qui l'entourent, il devient, au sein de ce réseau, un objet communiquant parmi d'autres dont certains vont entraîner telle ou telle réaction ;

- de l'abolition de la distinction entre **sphère publique et sphère privée**⁴⁵. L'homme perdu dans la foule peut être suivi, tracé. A l'inverse, même chez lui, enfermé à double tour, l'homme se voit à travers le GSM qu'il a en poche, les RFID qu'il peut porter, à travers son utilisation de la TV interactive, de son ordinateur relié à Internet, espionné, poursuivi et ses secrets d'alcôve percés. Nous reviendrons sur ce point. La protection du domicile physique, lieu inviolable, apparaissait traditionnellement et, aux yeux du droit, comme quelque chose de fondamental pour la construction de la personnalité de l'individu. Cette notion-là se trouve elle aussi bouleversée à l'heure actuelle par les développements technologiques.

En conclusion, on relève le risque déjà identifié dès 1983 par le Tribunal constitutionnel allemand⁴⁶ dans l'affaire du recensement statistique, d'une normalisation des comportements et des pensées des citoyens⁴⁷ édictée par la tyrannie d'un pouvoir informationnel diffus, insaisissable et à la puissance sans limites⁴⁸.

27. La question de l'autonomie se pose également au niveau collectif, c'est-à-dire des groupes et communautés. S'il est clair que sur le plan théorique, les technologies de l'information et de la communication facilitent leur présence et expression sur la toile et permettent de maintenir des identités culturelles, peu importe la distance, dans la pratique, il en est autrement : nos claviers, les URL ne peuvent exprimer toutes les langues et nombre de logiciels ne sont développés que dans les seules langues dominantes. Les deux sommets mondiaux de la société de l'information ont dénoncé cet état de fait⁴⁹ et certains efforts ont été entrepris mais les progrès sont lents et la Convention de l'UNESCO sur la reconnaissance de la diversité des expressions culturelles⁵⁰ risque sans cela de rester lettre morte.

2. Solidarité, justice sociale et ICT

28. Les valeurs de solidarité et justice sociale sont mises à mal dans le monde virtuel tout autant que dans le monde réel. A l'abri de tout contrôle social, sans vis-à-vis, l'internaute peut se laisser aller sous le masque du pseudonyme ou l'anonymat à des dérives de langages, à des comportements offensants ou choquants. La technologie l'aide à multiplier les spams, à s'introduire dans l'ordinateur d'autrui. Elle lui permet, à travers des opérations de forage des données (*data mining*⁵¹), de profiler autrui et, dès lors, de le manipuler, voire de ne point l'accueillir⁵².

29. Certaines logiques à l'œuvre derrière la sélection par les entreprises de leurs clientèles ou justifiant la fixation de conditions différenciées de transaction, même si elles sont justifiables économiquement, suscitent quelques appréhensions du point de vue des valeurs de solidarité et de justice sociale. Ainsi, les systèmes d'exploitation de données, non nécessairement à caractère personnel, permettent à un banquier de détecter des profils à risque en matière de crédits⁵³, à un assureur d'anticiper les risques liés à une catégorie tout à fait particulière d'individus et de discriminer ceux-ci.⁵⁴ L'appropriation croissante et parfois observée de l'information, à la fois, par l'exacerbation des droits de propriété intellectuelle et par les technologies de contrôle d'accès ou d'utilisation de l'œuvre, heurte ces mêmes impératifs de solidarité et justice sociale⁵⁵.

30. Enfin, on soulignera, après les deux sommets mondiaux de la société de l'information, les inégalités croissantes entre riches et pauvres, pays développés et pays sous développés, handicapés et non handicapés, groupes majoritaires et groupes marginaux et autres discriminations dans l'accès tantôt à l'infrastructure, tantôt à l'information, tantôt à

l'éducation, tantôt à l'ensemble de ces outils, en d'autres termes, on souligne le « *digital divide* », que provoquent ou, plutôt, accroissent les technologies de l'information et de la communication⁵⁶.

3. « Beneficence » et « maleficence » des technologies de l'information et de la communication

31. Suivant les réflexions souvent citées de Lessig⁵⁷, il est coutume de reconnaître que la technologie elle-même, son design et les choix qu'elle incorpore constituent en eux-mêmes des sources de régulation. Ainsi, les choix technologiques opérés qu'ils soient le fait d'une entreprise ou d'un organe de standardisation technique ne sont pas neutres, en particulier par les applications qu'ils autorisent.

A cet égard, nous avons déjà cité la façon dont la technologie des « cookies », fruit d'un standard mis au point par l'IETF, a pu être utilisée pour permettre le profilage des internautes et la manière dont les RFID sont devenus des instruments puissants de contrôle des déplacements, par exemple, d'employés ou de consommateurs. Le choix d'une technologie de signature unique, fût-elle fortement sécurisée, entraîne des risques potentiels de croisement des données résultant des différentes utilisations de la signature.

Les technologies dites de « *Digital Rights Management* » permettent de même un contrôle accru non seulement des accès aux œuvres, mais de l'utilisation de ces dernières⁵⁸. Les implants RFID dans le corps constituent une opportunité pour pallier certaines déficiences physiques ou pour soigner des maladies⁵⁹. Dans le même temps, elles engendrent des risques de surveillance et de manipulation à distance de l'individu et de ses affects. Bref, la technologie peut constituer un apport positif pour l'humanité comme elle peut mettre en péril les libertés des citoyens.

IV. De l'éthique aux droits de l'Homme

32. L'approche du Conseil de l'Europe en matière de droits de l'Homme et libertés se veut constructive et non simplement négative : « les droits de l'Homme et les libertés non seulement restreignent le pouvoir de l'Etat mais surtout ont pour but de mettre le citoyen en mesure de participer pleinement à la délibération collective. Ces droits et libertés rendent le citoyen capable de développer et d'exercer leur pouvoir de s'informer, de revoir et de poursuivre leur conception du bien... ». Cette conception des droits de l'Homme implique, nous l'avons dit, un rôle de l'Etat dans la mise en place des conditions qui permettent aux citoyens de jouer pleinement un rôle dans la société de l'information. Ces conditions visent non seulement les relations des citoyens avec l'Etat, mais également les relations des citoyens entre eux. Elle peut donc impliquer la mise à charge des pouvoirs privés de certaines obligations dans la mesure où celles-ci sont nécessaires à cet épanouissement personnel. Notre propos est d'épingler quelques devoirs qui nous paraissent s'imposer tant à l'Etat qu'aux organismes actifs dans la fourniture de biens et services de la société de l'information, afin de permettre le respect des valeurs éthiques que nous venons de développer.

A. De la dignité et l'autodétermination à la *Privacy* et à la protection des données à caractère personnel

33. Le « droit à la vie privée » (*The « right to Privacy »*) est conçu comme l'ensemble des prérogatives qui apparaissent nécessaires pour amener le développement de la personnalité de l'individu dans une société donnée et pour assurer ainsi la vitalité de nos sociétés démocratiques⁶⁰. Le « droit à la vie privée », s'il reste indéfinissable a priori, apparaît comme une condition structurante reconnue nécessaire par le droit à l'exercice possible de l'autonomie de l'individu. En ce sens, comme l'écrit H.BURKERT⁶¹, il constitue un droit « fondamental » dans la mesure où il conditionne l'exercice de l'ensemble des autres libertés et droits fondamentaux⁶². Par ailleurs, par l'exercice de cette autonomie rentre bien évidemment en conflit avec d'autres droits, libertés et intérêts des tiers et de l'Etat, dans la mesure où l'individu ne peut être considéré comme isolé mais au contraire situé dans des relations interpersonnelles et ce dans une société structurée. Il reviendra donc au juge de concrétiser la norme générale dans des situations concrètes⁶³. En ce sens, poursuit H.BURKERT, la vie privée est également un droit fondamentalement relatif.

34. Ce droit à la vie privée s'entend traditionnellement d'abord comme un droit négatif à l'intimité, c'est-à-dire les prérogatives qui permettent à l'individu de se protéger du regard d'autrui (protection du domicile comme endroit clos, de la famille et de la correspondance considérées comme espaces interpersonnels à l'abri des ingérences de l'autorité et des tiers) et à l'abri de ce regard, de pouvoir construire sa personnalité. C'est le « *Right to be left alone* » ou le droit à la « séclusion », selon la doctrine américaine⁶⁴. Progressivement à travers une jurisprudence de plus en plus hardie, la Cour de Justice de Strasbourg l'a étendu au droit, cette fois positif, reconnu à l'individu de pouvoir affirmer des choix essentiels, qu'il s'agisse de son nom, de ses identités et préférences sexuelles, de ses relations avec autrui et du choix de son lieu d'habitation⁶⁵, bref un droit au libre épanouissement de sa personnalité⁶⁶. Cette seconde facette du droit à la vie privée implique le droit de disposer des informations essentielles en matière de santé, sécurité, environnement et réglementation⁶⁷, et justifie un domaine public informationnel fort, capable de lui fournir les informations essentielles de manière à être capable de maîtriser – dans une certaine mesure au moins – l'environnement dans lequel il vit⁶⁸.

35. La jurisprudence du Conseil de l'Europe déduit de l'article 8 de la Convention européenne des droits de l'Homme non seulement une obligation négative de ne pas interférer avec la vie privée des citoyens mais en outre des **obligations positives** de l'Etat de mettre à disposition des citoyens les moyens de pouvoir exercer pleinement les prérogatives liées au respect de cette autonomie et des diverses facettes de cette autonomie tant dans les relations du citoyen avec l'Etat mais également dans la relation qu'il entretient avec les autres citoyens (**effet dit horizontal de la CEDH**⁶⁹). La Cour de Strasbourg se réserve le droit d'examiner si l'Etat, par omission ou par action, a maintenu un « juste équilibre » entre, d'une part, l'intérêt général, les différents droits et intérêts en présence et, d'autre part, l'intérêt de l'individu à la protection de sa vie privée entendue au sens le plus large⁷⁰.

36. C'est précisément au vu de cette obligation positive de l'Etat que l'irruption du fait technologique a rendu nécessaire l'intervention législative des Etats en matière de protection des données à caractère personnel. L'utilisation de plus en plus massive de données à caractère personnel et leur traitement par des outils logiciels de plus en plus performants constituent des risques nouveaux pour l'autodétermination de chacun. On a déjà noté les risques de réductionnisme associés au profilage des personnes et, partant, les risques de

discrimination ou simplement d'erreurs qui en découlent. On a déjà suggéré le déséquilibre informationnel existant entre les responsables de traitement (entreprises, associations et administrations) et la personne concernée. On a enfin évoqué l'opacité des traitements et en tout cas des raisonnements à l'œuvre derrière ces traitements, générateurs de normalisation et exposant la société au risque d'un « conformisme anticipatif » de la population, dénoncé dès 1983 par le Tribunal constitutionnel allemand de Karlsruhe. Tous ces éléments empêchent les personnes de participer pleinement à la vie sociale et d'y apporter leur contribution originale. La Convention n°108 du Conseil de l'Europe relaie cette préoccupation en faisant « *peser une responsabilité sociale accrue sur les acteurs publics et privés* »⁷¹ et en affirmant les principes de transparence, de proportionnalité et de sécurité comme fondements même des initiatives législatives en la matière. Il s'agit à travers ces législations de créer un certain droit de contrôle individuel et collectif sur la circulation de l'image informationnelle. En d'autres termes, les législations de protection des données apparaissent comme un « moyen » dérivé du droit à la protection de la vie privée, pour assurer la protection des valeurs éthiques de dignité et d'autonomie personnelle⁷² et ce dans un contexte donné : celui du développement des technologies de l'information et de la communication.

37. Les écrits de LESSIG⁷³ et de REIDENBERG⁷⁴ parmi d'autres attirent notre attention sur la nécessité de tenir compte, dans la protection de la vie privée que nous voulons garantir, de l'architecture du système dans lequel nous évoluons et surtout de son évolution. Les règles affirmées dans une société où les traitements de l'information nominative venaient de voir le jour doivent donc être réévaluées aujourd'hui à l'aune de la dimension ubiquitaire, globale et interactive de nos réseaux et des systèmes d'intelligence ambiante. Ainsi à l'heure où la technologie ubiquitaire trace chacun de nos gestes et choix, fussent-ils les plus instantanés, et pénètre nos foyers, il est important que de nouveaux droits soient affirmés : celui d'une protection de la « *virtual home* » au-delà de la « *physical home* », celui de la maîtrise et de la transparence de nos terminaux, celui de se déconnecter et d'utiliser un pseudonyme dans nos communications avec autrui⁷⁵.

Le droit de s'opposer aux communications non sollicitées participe également de ce même souci de ne pas être victime d'intrusions et d'être laissé seul. Par ailleurs, ce droit s'explique également par la volonté de ne pas être réduit à son profil et confirmé dans celui-ci, sans plus de possibilité d'être surpris et invité au changement.

38. Certains de nos gestes parce qu'ils sont triviaux ou parce qu'ils répondent à une sollicitation instantanée sont conçus comme ne laissant pas de traces (si ce ne sont celles recueillies éphémèrement ou non, consciemment ou non par un voisin). La technologie actuelle permet de collecter ces informations, de les traiter et d'en déduire, connectées ou non à d'autres informations, des profils de personnalité permettant d'agir vis-à-vis des personnes concernées. Par leur enregistrement et leur conservation, les traces précédemment volatiles par excellence de nos activités et comportements les plus anodins revêtent à présent du sens, dans la mesure où elles sont interprétées, seules ou en relation avec d'autres traces tout aussi anodines par elles-mêmes mais néanmoins enregistrées. Les individus n'ont le plus souvent aucun contrôle sur le sens qui est ainsi produit, sur la construction du « savoir » qui pourtant les concerne. Ils n'ont d'ailleurs que très peu conscience de l'existence de ces constructions tant leurs « *expectations of privacy* »⁷⁶ sont en décalage avec la situation réelle dans laquelle ils se trouvent (c'est en tout cas le cas en ce qui concerne des gestes et comportements auxquels eux-mêmes n'attachent aucune signification). Dans le contexte de certains systèmes d'intelligence ambiante, les personnes se voient réduites à devenir, au sein des réseaux qui les entourent, purs objets en relation avec d'autres objets qui interagissent avec eux.

39. Si l'autodétermination individuelle est une condition⁷⁷ qui représente un élément structurant pour notre participation dans une société démocratique, l'approche en termes de propriété par le sujet de ses données à caractère personnel est à rejeter⁷⁸. De même, si le consentement peut à juste titre être considéré comme une des conditions nécessaires de légitimité des traitements, il ne peut, au contraire de ce qu'affirment certaines théories néolibérales être une cause suffisante de légitimité. Ce point est important dans la mesure où la technologie crée l'illusion en tout cas d'un possible « user empowerment » (PICS, P3P) où l'internaute serait lui-même apte à décider des traitements qu'il autorise⁷⁹. La doctrine du consentement comme fondement suffisant du traitement des données ne prend en compte ni la question des « capabilities »⁸⁰ dans la société de l'information, le fait que les nécessités ou avantages liés à la vente de données peuvent être attractifs pour des personnes fragiles socio-économiquement parlant, ni l'effet « dominos », c'est-à-dire le fait que la divulgation volontaire par une personne de 'ses' données personnelles 'force' les autres à donner la même information, sous peine de suspicions envers eux⁸¹.

Par ailleurs, la technologie permet dans de nombreux secteurs de développer des mécanismes décisionnels « one-to-one » fondés sur l'accumulation de données qui permettent un profilage fin. Cette pratique pose deux questions. Premièrement, peut-on admettre la prise en considération de n'importe quelle donnée même si son utilisation dans une perspective de rationalité économique le justifie (exemple : la situation de violence conjugale dans laquelle vivrait une personne peut-elle être prise en compte pour le calcul actuariel d'une prime d'assurance-vie) ? Ne faut-il pas obliger les décideurs à mieux expliciter leurs critères de décision et permettre une négociation collective et le cas échéant arbitrée par une autorité sur la proportionnalité de ces systèmes ? Seconde question, il est important de rappeler aujourd'hui le principe de la compatibilité des traitements, fondés en définitive sur la question de l'intégrité contextuelle⁸², la personne donne son information dans un contexte donné et s'attend raisonnablement qu'elle soit traitée dans ce contexte, sous peine de risquer d'être jugée « hors contexte ».

40. Le caractère global de nos réseaux et l'importance des risques pour l'autonomie individuelle du fait même des technologies à l'œuvre au sein de ces réseaux amènent à prôner une reconnaissance globale des règles de protection des données. Lors de sa réunion de Tunis, le Sommet mondial de la société de l'information a appelé de ses vœux la définition d'une charte globale en matière de Privacy devant trouver dans des modes divers de régulation adaptés à chaque culture son expression. La Convention n° 108 pourrait apparaître, sur le modèle de la Convention sur la cybercriminalité ouverte avec succès à des pays non-membres du Conseil de l'Europe, comme la base sur laquelle pourrait se construire ce consensus mondial.

41. Une dernière remarque ouvre le débat sur l'intérêt d'une reconnaissance non seulement individuelle de l'autonomie mais également collective. L'importance consacrée par les lois de protection des données de la transparence des traitements et du contenu informationnel sur lesquels ces traitements s'appuient comme condition du respect de l'autonomie de chacun ne doit-elle pas également être affirmée vis-à-vis des collectivités et des Etats ? On connaît le cas célèbre de cet Etat africain dont les ressources du sous-sol étaient mieux connues par des entreprises à la recherche de nouveaux lieux d'exploitation des ressources du sous-sol que par le gouvernement local. Ne doit-on pas considérer qu'il existe pour les collectivités comme pour les Etats, un droit d'accès aux données les concernant, dans la mesure où ces données sont essentielles pour leur assurer la maîtrise de leur développement ?

B. Liberté d'expression comme conséquence du principe d'autonomie : quelques considérations sur sa signification individuelle et collective dans la société de l'information

42. Le développement de la société de l'information accroît les chances de chacun et de chaque collectivité de pouvoir s'exprimer librement dans le cyberspace et de pouvoir recevoir l'information nécessaire à l'exercice de ses prérogatives de citoyen, de collectivité et d'Etat. La liberté d'expression sur l'Internet a été rappelée récemment par le Comité des Ministres du Conseil de l'Europe dans sa déclaration du 28 mai 2003⁸³. Si à cet égard l'Internet remplit la plupart de ses promesses, on sera attentif aux risques et aux conditions d'un accès de tous à cette liberté d'expression. Les points précédents consacrés au droit à la protection de la vie privée comme traduction juridique des exigences consacrées au titre de l'autodétermination, mettaient en évidence le fait que sans la reconnaissance de ce droit à la protection de la vie privée, l'affirmation de la liberté d'expression serait illusoire. Il est évident que la condition d'une expression totalement libre renvoie à notre capacité d'autodétermination, à ce sentiment de non-surveillance et de non-opacité des traitements qui concernent les données qui résultent de notre prise de parole ou y sont contenues. Oserais-je signer une pétition en faveur de telle cause généreuse si je crains que, demain, un moteur de recherche puissant offre à un futur potentiel employeur les moyens de me stigmatiser pour cette prise de position? A ce propos, la seule consécration constitutionnelle de la liberté d'expression sans la consécration conjointe ou première du droit à la protection de la vie privée est, à notre sens, insuffisante.

43. Au-delà, on évoque deux conditions préliminaires, nécessaires, à la liberté d'expression : la première tient au droit de chacun de disposer d'une éducation qui le rende apte à pouvoir s'exprimer dans le cyberspace. Nous reviendrons sur ce point lorsque nous évoquerons à propos de la valeur de solidarité et de justice sociale⁸⁴, les diverses composantes de la notion d'accès universel. La seconde condition tient cette fois à la nécessité de maintenir un juste équilibre entre les intérêts des créateurs des œuvres informationnelles et ceux qui souhaitent y accéder. Sans doute, et on le rappelle avec force, les droits d'auteur trouvent leur fondement ultime dans la liberté d'expression consacrée par l'article 10 de la Convention européenne des droits de l'Homme⁸⁵ mais l'autre versant de cet article 10 qui souligne le droit de recevoir l'information implique que les droits de propriété intellectuelle ne puissent en réserver l'utilisation et la jouissance qu'aux seuls nantis, tant par la force de la réglementation que par les technologies qui permettent d'enfermer l'œuvre mieux que dans un coffre-fort⁸⁶. On a déjà souligné à cet égard l'intérêt des mouvements d'« *open source* » ou d'« *open document* », qui méritent évidemment d'être encouragés⁸⁷.

44. La lutte contre la circulation de messages illicites ou dommageables et le souci louable de protéger notre jeunesse peuvent conduire à des censures d'autant plus dangereuses qu'elles sont le fait non plus de l'autorité publique dans le cadre de procédures bien connues mais d'acteurs privés au premier rang desquels on note les hébergeurs, les fournisseurs d'accès et les moteurs de recherche, ceux qu'il est coutume de qualifier : « *les gatekeepers* ». On veillera donc à ce que, d'une part, les règles de responsabilité pour l'information transmise, hébergée ou sélectionnée ne conduisent pas ces derniers à réguler l'expression dans le cyberspace et que d'autre part, les opérations, par lesquelles ces « *gatekeepers* » pourraient restreindre l'accès à l'information ou la manipuler, soient totalement transparentes et soumises à un contrôle démocratique. Il ne peut être question de confier le contrôle de l'information qui circule dans le cyberspace à des instances auto-régulées ne fonctionnant pas sur des valeurs

universelles. Les principes de neutralité et de transparence vis-à-vis des citoyens doivent en tout état de cause être imposés lorsque ces intervenants sont de fait incontournables.

45. La signification collective du droit à la dignité et à l'autonomie aboutit également, en matière de liberté d'expression, à reconnaître à chaque peuple la capacité de pouvoir exprimer son identité culturelle (ce qui est une question de langue mais au-delà de manifestations culturelles propres) sur la toile et de pouvoir participer ainsi à la construction de l'héritage commun de l'humanité. De la même manière que l'autonomie individuelle s'impose comme un bien collectif, condition d'une démocratie vivante, fondée sur le respect des différences et riches de celles-ci, l'autonomie des peuples apparaît comme contributive à la richesse du patrimoine commun de l'humanité⁸⁸.

C. De la solidarité et de la Justice sociale

46. Internet, nous l'avons dit (supra n° 27) de par ses caractéristiques multiplie les risques d'atteintes au respect d'autrui et à la sécurité collective. L'existence de tels risques justifie sans doute l'intervention de l'Etat dans les strictes limites du respect d'autres valeurs, en particulier celles de l'autonomie qui renvoie en droit tant à la protection de la vie privée que de la liberté d'expression. En d'autres termes, si la lutte contre la criminalité informatique trouve dans l'existence de ces risques sa justification, le rappel de la valeur supérieure que constitue l'autodétermination fixe à cette lutte des limites. Il ne peut être question de proclamer, comme le font certains partisans d'une société de la surveillance, un prétendu droit autonome à la sécurité à placer sur le même pied que la liberté fondamentale que consacre le droit à la protection de la vie privée et que prolonge la liberté d'expression et de réception de l'information. Les articles 8 et 10 de la CEDH imposent que les mesures prises en la matière soient consacrées par des lois claires et précises, et « nécessaires dans une société démocratique ». La Convention du Conseil de l'Europe sur la cybercriminalité du 15 novembre 2001⁸⁹ a cherché à fixer les contours des pouvoirs nouveaux d'investigation, justifiés par la nature particulière de l'Internet et des risques qui lui sont spécifiques. Les auteurs du présent rapport notent que depuis la Convention se sont multipliées les lois et pratiques qui étendent les pouvoirs d'investigation des pouvoirs publics⁹⁰ voire privés⁹¹ bien au-delà des contours tracés par la Convention. Le débat sur leur nécessité dans une société démocratique est escamoté⁹² et il n'est proposé aucune évaluation ni de leur efficacité pour la prévention et la poursuite des crimes et délits, ni de leur impact sur l'autodétermination. C'est bien ce manque de « contrôle des contrôleurs », plus qu'un soi-disant conflit entre les valeurs de la vie privée et de la sécurité, qui pose problème. Afin de bien peser les enjeux, posons qu'il ne s'agit pas d'opposer les objectifs de sécurité et de protection de la vie privée, ce serait manquer la cible. Ce dont il est question, derrière ces débats actuels, dont les termes sont trop souvent mal identifiés, c'est d'une opposition bien plus fondamentale entre les conditions d'un état démocratique (qui ne sont pas incompatibles avec un certain niveau de surveillance et de contrôle, mais où cette surveillance et ce contrôle sont eux-mêmes décidés démocratiquement, et sont appliqués suivant des règles et en fonction d'objectifs déterminés, eux aussi, démocratiquement) et les conditions d'un état totalitaire (pas plus incompatibles bien entendu, avec la surveillance et le contrôle mais qui cette fois ne sont ni délibérés, ni contrôlés démocratiquement).

47. En outre, la volonté de permettre à chacun de pouvoir s'exprimer sur le Net oblige l'Etat à développer une politique d'accès universel de manière à lutter contre la fracture numérique, sous peine de quoi la liberté d'expression et de réception resterait un vœu sans lendemain. On insiste⁹³ sur le fait que le service universel ne s'entend pas uniquement d'un accès à une

infrastructure de qualité permettant un accès aisé à la toile, d'un accès global et sans doute via des infrastructures appropriées aux particularités tant géographiques que de développement des diverses communautés. Il s'élargit au besoin de doter des lieux ouverts au public de moyens d'accès qui permettent à des collectivités rurales n'ayant pas les moyens financiers de connexion individuelle de pouvoir s'exprimer et bénéficier des ressources du Net, ce qui implique comme corollaire le droit de chacun de recevoir une éducation à l'utilisation de l'Internet; il nécessite, comme le note l'agenda de Tunis du Sommet mondial de la société de l'information, de développer un véritable service public informationnel relatif à des données essentielles au citoyen (données réglementaires, informations juridiques, de santé, de sécurité, données relatives à la conduite des affaires publiques ...), dont le développement se justifie en considérant que le droit d'accès⁹⁴ aux documents du service public doit tenir compte des facilités offertes par les technologies de l'information et de la communication et implique dès lors une politique active de diffusion par l'Etat des données dont il dispose⁹⁵. Enfin, on s'interroge sur la nécessité de reconnaître des lieux d'hébergement publics ou d'imposer l'obligation pour des opérateurs de plateforme d'héberger les sites de collectivités qui ne pourraient trouver sur l'Internet la possibilité de s'exprimer que ce soit pour des raisons de maîtrise technologique ou simplement eu égard aux coûts d'hébergement. Cette idée a été développée dans certains pays, en particulier dans certains Etats des Etats-Unis à propos du droit des collectivités minoritaires de pouvoir bénéficier d'une place sur le câble (sorte de « *must carry* ») pour diffuser leurs programmes audiovisuels. Elle pourrait s'avérer utile dans le cadre de l'Internet.

48. La justice sociale exige également que des précautions soient prises de manière à lutter contre certains traitements du secteur privé, qui pourraient permettre d'exclure des catégories de population de l'accès à des services essentiels comme le logement, certains services d'assurance ou bancaires, etc.. Nous avons noté (supra, n°27) le fait que des utilisations de la technique de *data mining* peuvent avoir pour effet une telle discrimination qui, même si elle est économiquement rationnelle dans le chef du responsable du traitement, soulève des questions essentielles de société et de cohésion sociale. On note que les mêmes risques d'exclusion sont liés à l'existence de listes noires.

D. « Beneficence » et « non maleficence »

49. Le développement technologique lui-même est questionné par les valeurs éthiques. Il est clair que les choix technologiques recèlent par les applications qu'ils permettent des atteintes à ces valeurs. Ainsi, certaines applications RFID qui permettraient des manipulations à distance du cerveau humain peuvent être jugées incompatibles avec la dignité de l'homme. Récemment lors des débats aux Etats-Unis à propos de l'insertion d'une puce RFID dans le passeport des citoyens, les fabricants de puces eux-mêmes ont attiré l'attention sur les risques liés à une telle insertion et ont souligné l'atteinte à la confiance que le déploiement de cette application allait entraîner auprès de citoyens craignant d'être surveillés sans répit⁹⁶. On peut ainsi multiplier les exemples.

Par rapport à ce constat, le rôle du droit semble être double : La loi peut poser certaines exigences relatives au développement des systèmes technologiques. Le droit ne se contente pas d'encadrer la technologie, il peut exiger que le design même des systèmes technologiques soit conforme aux prescrits légaux et réglementaires⁹⁷. Il peut, au-delà, promouvoir les technologies qui apportent une plus-value à la défense des droits fondamentaux⁹⁸ et combattre les technologies qui mettent en cause ces derniers.

Ainsi, prenons le cas de la technologie des RFID et l'application des lois en particulier de protection des données : l'accès aux données contenues dans une puce RFID par une borne de lecture placée par une personne non autorisée constitue un hacking⁹⁹, de même que l'interception des données transmises par un RFID à une borne située à distance est punissable. On insiste sur la nécessité tant pour les concepteurs des applications de cette technologie que pour ceux qui les utilisent d'entourer les dispositifs de transmission et les produits RFID d'une sécurité appropriée. Ainsi, le cryptage automatique des transmissions, les contrôles d'accès à la puce sont autant de mesures que les obligations de sécurité déduites des législations de protection des données imposent¹⁰⁰. Voilà qui met en évidence la part de responsabilité des fabricants relativement au principe général du respect de la vie privée. Cette responsabilité se déduit du considérant 2 de la Directive européenne 95/46 : « *les systèmes de traitement sont au service de l'homme... doivent respecter les libertés et droits fondamentaux des personnes, notamment la vie privée ... doivent contribuer au progrès économique et social et au bien-être des individus* ». Cette **responsabilité des fabricants des produits technologiques** et des concepteurs des applications de la technologie a été soulignée à plusieurs reprises par le Groupe dit de l'article 29. L'article 14, alinéa 3 de la directive 2002/58 lui donne une première concrétisation lorsqu'elle affirme : « *Au besoin, des mesures peuvent être adoptées afin de garantir que les équipements terminaux seront construits de manière compatible avec le droit des utilisateurs de protéger et de contrôler l'utilisation de leurs données à caractère personnel...* ». Sans doute, faut-il voir dans ce prescrit la volonté délibérée de l'Europe d'exiger une technologie « *privacy compliant* », c'est-à-dire intégrant dans sa modélisation et son fonctionnement les conditions d'un respect des législations en matière de protection des données. Comme le notait R.Clark¹⁰¹ à propos des dangers que court le respect des droits de la propriété intellectuelle du fait des nouvelles technologies, c'est au sein de la technologie que doivent être trouvées les solutions aux risques créés par cette technologie.

50. Elargissons le débat : la réflexion éthique et l'analyse des impacts de l'innovation technologique doivent être prises en compte dès le début du développement de la technologie. On insiste donc sur l'importance d'une telle réflexion et analyse au sein des organes de standardisation qui définissent les normes techniques¹⁰². C'est au droit à mettre en place, suivant le principe de précaution, des procédures qui obligent à une réflexion ouverte à laquelle doivent prendre part les différents acteurs intéressés au développement de la technologie. L'application du principe de précaution¹⁰³ tout comme celui de la responsabilité partagée des producteurs de technologies à raison du risque créé, principes chers au droit de l'environnement¹⁰⁴ se justifient aisément par l'importance des risques encourus par nos sociétés du fait de ces technologies. Internet n'est-il pas également un écosystème mis en danger par certaines pratiques et technologies ? Les principes de transparence et de délibération « *multi-stakeholders* » affirmés notamment par la Convention d'Aarhus¹⁰⁵ trouveraient dès lors un écho.

CONCLUSIONS

51. Notre propos était de rappeler l'importance des valeurs éthiques dans la société de l'information et ce sous les auspices du Conseil de l'Europe et de l'UNESCO. L'identification de valeurs éthiques universelles est absolument nécessaire si nous voulons promouvoir un Internet global qui respecte la diversité et les richesses culturelles, tout en favorisant la participation de chacun, et de chaque communauté, aux bénéfices culturels, informationnels, économiques, politiques et de communication rendus possibles dans la société de

l'information. La recherche de ces valeurs se justifie également par le fait que les technologies de l'information façonnent, de manière de plus en plus incontournable, le mode de notre vivre ensemble, collent à notre peau, à nos déplacements, à nos choix qu'ils soient triviaux ou essentiels et conditionnent de plus en plus le déroulement de nos vies.

Ces valeurs éthiques renvoient, on le pressent, à une multiplication des lieux où les acteurs se réapproprient les valeurs dûment contextualisées, que ce soit par exemple des jeunes lorsqu'ils mettent en place un forum de discussion, une association de libraires, un laboratoire de recherches mettant au point une application nouvelle en matière d'intelligence ambiante ou Google, à propos des services associés à son moteur de recherche. Ce relais par des éthiques particulières permettra la traduction de valeurs abstraites en « *best practices* », des codes de conduite, des solutions techniques qui contribueront dans des contextes particuliers à reconnaître la dignité de chacun, à se soucier des conditions d'un développement réellement personnel et témoigneront des valeurs de solidarité et de justice sociale.

52. L'assertion des valeurs éthiques n'est pas suffisante. Elle doit se prolonger par une affirmation des libertés et droits fondamentaux qui traduisent ces valeurs éthiques. En particulier, il nous apparaît central que soit assurée la protection de nos vies privées dans toutes les facettes que progressivement la jurisprudence du Conseil de l'Europe a consacrées. Cette consécration juridique garantit notre « auto-détermination informationnelle », dont le maintien est sans doute l'un des enjeux principaux pour l'avenir de notre société de l'information. Il importe dès lors que, sur base de la Convention n°108, le Conseil de l'Europe se fasse le champion de l'adoption d'un instrument global de protection des données. Le Conseil rappellera cet enjeu majeur au sein des discussions internationales en particulier dans le cadre de l'*Internet Governance Forum*, mis en place à la suite du Sommet de Tunis sur la société de l'information et dont la première réunion s'est tenue à Athènes.

Au-delà de cette consécration de la « vie privée », le rapport souligne la transformation profonde des acteurs et du fonctionnement de l'espace public de discussion ; cette transformation exige une réflexion renouvelée sur la régulation des médias. Les valeurs de solidarité et de justice sociale doivent amener l'Etat certes à lutter contre la cybercriminalité mais surtout à veiller positivement à ce que chacun dispose des moyens y compris de l'éducation pour s'exprimer sur la toile et ne puisse se voir exclu par des utilisations illégitimes de services ou biens essentiels. C'est à l'Etat, au besoin par la proclamation de droits nouveaux, d'assurer les conditions d'effectivité des libertés individuelles et collectives fondamentales.

53. Parmi ces conditions d'effectivité, on est attentif au fait que la technologie elle-même, loin d'être neutre, est un facteur de régulation du comportement des acteurs et de leurs relations. C'est sur cette base que nous avons plaidé pour l'extension des principes de précaution et de responsabilité partagés de ceux qui effectuent ces choix technologiques. Ces choix se doivent d'être conformes, voire promouvoir les choix normatifs auxquels les citoyens ont donné leur assentiment. Ainsi il est plaidé non seulement pour un « *value sensitive design* » de la technologie qui rejoint la nécessité d'une technologie « *democracy sensitive* », c'est-à-dire résultant d'une délibération démocratique entre les différents « *stakeholders* » et en même temps cherchant à accroître une participation démocratique et l'inclusion de tous dans la vie de la société.

¹ Recommandation sur la Promotion et l'usage du Multilinguisme et l'Accès Universel au Cyberespace, texte adopté par la Conférence générale de l'UNESCO à sa 32ème session (Octobre 2003)

² Convention sur la protection et la promotion de la diversité des expressions culturelles, adoptée par l'assemblée générale de l'UNESCO, Paris, le 20 octobre 2005. La Convention sur la protection et la promotion des expressions culturelles vise à renforcer les liens qui unissent culture et développement durable, et à mettre en place une approche novatrice de la coopération internationale. Elle réaffirme le respect des droits de l'Homme et des libertés fondamentales, l'égalité des cultures, l'accès équitable et l'ouverture des cultures au monde. À ce jour, elle compte 76 Parties : 75 États et la Communauté européenne, qui a ratifié le texte en tant qu'organisation d'intégration économique régionale.

La Convention reconnaît la nature spécifique des activités, biens et services culturels en tant que porteurs d'identité, de valeurs et de sens. Elle reconnaît donc aux États le droit de formuler des politiques qui favorisent l'épanouissement de la diversité des expressions culturelles sur leurs territoires et encouragent l'accès équitable à toutes les expressions culturelles du monde. Aussi, les Parties à la Convention s'engagent à faciliter les échanges culturels à l'intérieur des frontières ainsi qu'avec les autres pays.

³ Déclaration universelle sur la bioéthique et les droits de l'Homme, 19 octobre 2005.

⁴ Conseil de l'Europe, Convention de sauvegarde des droits de l'homme et des libertés fondamentales, Convention adoptée le 4 novembre 1950. La structure des articles 8 et 10 auxquels le texte fait référence est semblable. L'alinéa 1 affirme la liberté et l'alinéa 2 prévoit la possibilité d'exceptions soumises à des conditions de légalité, de précision et de proportionnalité par rapport à des objectifs déterminés (sécurité publique, droits et libertés d'autrui, etc.).

⁵ Convention pour la protection des personnes à l'égard du traitement automatisé de données à caractère personnel, Strasbourg, STE n° 5, 28 janvier 1981. Cette Convention a été suivie de nombreuses recommandations sectorielles, en particulier la Recommandation n° R (99) 5 contenant les lignes directrices pour la protection de la vie privée dans l'Internet.

⁶ Recommandation CM/Rec(2007)11, du Comité des Ministres sur la promotion de la liberté d'expression et d'information dans le nouvel environnement de l'information et de la communication, adoptée le 28 septembre 2007. Cf. également les déclarations du Conseil des Ministres de 2003 sur la liberté d'expression sur l'Internet et de 2005 sur les droits de l'Homme et l'Etat de droit dans la société de l'information.

⁷ « The Convention is deemed a “*living instrument*”, which ought to be interpreted only in an extensive way”. , R.A. LAWSON, “The monitoring of Fundamental Rights in the Union as a Contribution to the European Legal space : the role of the European Court of Justice”, dans *Proceedings of the first REFGOV Open Conference*, O. de SCHUTTER (ed.), mai 2006, Bruxelles, en voie de publication. L'auteur se réfère en particulier aux attendus de la Cour dans les cas *Tyrer* et *Selmouni*.

⁸ La Convention du Conseil de l'Europe met à charge de l'Etat non seulement des obligations négatives, celles de ne pas entraver le développement des libertés et droits fondamentaux que la Convention reconnaît mais en outre des obligations positives, celles de mettre en place les conditions, au moins minimales et compte tenu des spécificités et sensibilités propres de chaque Etat, de l'épanouissement de ces libertés et de ces droits. Sur ces obligations positives de l'Etat dans la jurisprudence de la Cour européenne des droits de l'Homme, lire parmi bien d'autres, F.SUDRE, « *Rapport introductif* », in *Le droit au respect de la vie privée au sens de la Convention européenne des droits de l'Homme*, op. cit., p.25 et s. Voir aussi, l'arrêt *Refah*, 2003 : « « *the State has a **positive obligation** to ensure that everyone within its jurisdiction enjoys in full, and without being able to waive them, the rights and freedom guaranteed by the Convention* ».

⁹ S. VAN DROOGHENBROECK, « L'horizontalisation des droits de l'Homme », in H. Dumont, F. Ost, S. Van Drooghenbroeck (dir.), *La responsabilité, face cachée des droits de l'Homme*, Bruxelles, Bruylant 2005, pp. 355-390 ; voy. aussi J. MOULY, « Vie professionnelle et vie privée. De nouvelles rencontres sous l'égide de l'article 8 de la Convention européenne des droits de l'homme », in F. Sudre (éd.), *Le droit au respect de la vie privée au sens de la Convention européenne des droits de l'Homme*, Bruxelles, Bruylant, Némésis, 2005, pp. 279-303, spéc. n° 13.

¹⁰ Le lecteur se référera pour un exposé plus complet à l'ouvrage de M. RUNDLE et C. COWLEY, « *Ethical Implications of Emerging Technologies : A. Survey* », IFAP, UNESCO, Paris, 2007.

¹¹ RFID : radio frequency identification technologies

¹² Sur ces premières applications et la valeur ajoutée de la technologie RFID par rapport aux codes-barres, lire G.T. FERGUSSON, « Have your Objects call my Objects », *Harv. Business Rev.*, 80 (6), p.138-144 ; D. DARQUENNES-Y. POULLET, RFID : Quelques réflexions introductives à un débat de société, *RDTI*, 2007, p. 255-285. Sur cette évolution des applications, lire J.BOHM, V. GROAMK, M.LANGHEINRICH, F. MATTERN, M. ROBS, « Living in a World of Smart everyday Objects – Social, Economic and Ethical Implications », 10 *Journal of Human and Ecological Risk*, 5, Oct.2004, p. 763-786 et M. VAN DE VOORT et A.LIGTVOET, Towards an RFID policy for Europe, Workshop Report, 31 août 2006, document préparé pour la DG INFSO à la suite des ateliers organisés par la Commission européenne les 15, 16 et 17 mai 2006, en particulier le chapitre 3.

¹³ La Directive 98/44/CE du Parlement européen et du Conseil du 6 juillet 1998 relative à la protection juridique des inventions biotechnologiques, (*Journal officiel n° L 213 du 30 juillet 1998 p. 0013 – 0021*), prévoit ceci : Article 6 : 1. Les inventions dont l'exploitation commerciale serait contraire à l'ordre public ou aux bonnes mœurs sont exclues de la brevetabilité, l'exploitation ne pouvant être considérée comme telle du seul fait qu'elle est interdite par une disposition légale ou réglementaire. 2. Au titre du paragraphe 1 ne sont notamment pas brevetables: a) les procédés de clonage des êtres humains; b) les procédés de modification de l'identité génétique germinale de l'être humain; c) les utilisations d'embryons humains à des fins industrielles ou commerciales; d) les procédés de modification de l'identité génétique des animaux de nature à provoquer chez eux des souffrances sans utilité médicale substantielle pour l'homme ou l'animal, ainsi que les animaux issus de tels procédés.

¹⁴ Sur cette loi et ses conséquences en matière de protection des données, lire Y.POULLET et J.M. DINANT, « L'autodétermination informationnelle à l'ère de l' Internet », Eléments de réflexion sur la Convention n° 108 destinée au travail futur du Comité consultatif (T-PD), Rapport publié sur le site du Conseil de l'Europe, http://www.coe.int/T/F/Affaires_juridiques/Coopération_juridique/Protection_des_données/

¹⁵ Pour d'autres exemples et des chiffres, lire Y. POULLET et J.-M. DINANT, « Self determination in an Information Society », Rapport au comité consultatif de la Convention n° 108, Conseil de l'Europe, novembre 2004, rapport cité note précédente.

¹⁶ Sur le « Web sémantique », la vision de T.BERNEERS LEE, "I have a dream for the Web [in which computers] become capable of analyzing all the data on the Web – the content, links, and transactions between people and computers. A 'Semantic Web', which should make this possible, has yet to emerge, but when it does, the day-to-day mechanisms of trade, bureaucracy and our daily lives will be handled by machines talking to machines. The '[intelligent agents](#)' people have touted for ages will finally materialize".

¹⁷ T. OLSEN, T. MAHLER et alii, *Privacy and Identity Management*, Complex 4/07, Oslo.

¹⁸ Sur l'intelligence ambiante aussi qualifiée d' "Ubimedia" lire, A. GREENFIELD, *Every(ware) ,the Ubimedia revolution*, New Riders/Peachpit- Pearson Ed. Group, 2006. Le terme est utilisé pour la première fois en 1999 par le Groupe consultatif du programme IST de l'Union européenne (L'ISTAG) dans son rapport sur le futur des technologies. Sur tout cela J. AHOLA, « Ambient Intelligence », *ERCIM News*, 2001, n° 47, disponible sur le site : http://www.ercim.org/publications/Ercim_News/enw47 .Cf. également l'expression « d'Ubiquitous Computing » lancée dès 1991 par M. WEISER, « The computer for the 21st Century », *Scientific American*, 265 (3), p. 66 à 75.

¹⁹ Selon la vision prophétique de WEISER (cité note précédente) qui, en 1991, affirmait : « les technologies les plus profondes sont celles qui disparaissent. Elles pénètrent dans la vie quotidienne à tel point qu'elles ne s'en distinguent plus. Elles sont invisibles ».

²⁰ Sur les nouveaux défis que représente la nanotechnologie, lire L.CAMPBELL, « Nanotechnologies and the U.S. National Plan for Research and Development in Support of Critical Information Protection », *Canadian Journal of Law and Technology*, vol.5, no.3, novembre 2006.

²¹ En matière de santé, on étudie également l'implant de radio-tags sur les humains (La Société Applied Digital Solutions et sa puce Verichip). Ces solutions peuvent être très utiles pour certaines catégories de patients à risque (Alzheimer ou souffrant de problèmes cardio-vasculaire ou encore de diabète), dans la mesure où on pourrait insérer dans la puce les données médicales dites d'urgence, ce qui permettrait en cas de besoin d'intervention vis-à-vis d'un patient incapable de s'exprimer, de lire à distance la puce et de connaître les contre-indications

que révèlent ces données d'urgence. Le récent rapport du Groupe européen d'Éthique de la Santé (Avis du Groupe européen d'Éthique des Sciences et des nouvelles technologies auprès de la Commission européenne, « *Aspects éthiques des implants TIC dans le corps humain* », 16 mars 2005) décrit ainsi nombre d'applications dont l'intérêt médical est, dans la plupart des cas, évident. Ainsi un implant dans le corps d'un patient à maladie chronique comme le diabète permet de contrôler à distance via le téléphone l'état du patient diabétique voire, dans le cadre d'un RFID interactif, de lui envoyer les impulsions nécessaires à un rétablissement de la situation compromise.

²² Cf. le célèbre cas de la discothèque Baja Beach Club implantée aux pays Bas et en Espagne (<http://www.baja.nl>) sans ancrage nécessaire dans un territoire donné et surtout sa nature.

²³ « La production et l'application du droit selon ses modes traditionnels se trouvent profondément mises en cause dans le cyberspace du fait même de ses caractéristiques. Là où l'État national imposait le droit, dans le cadre de compétences clairement définies par nos Constitutions et se réservait grâce au pouvoir judiciaire le quasi-monopole de son interprétation, le caractère global de l'Internet, son infrastructure totalement décentralisée, ses activités dématérialisées interactives remettent profondément en cause les schémas traditionnels de réglementation fondée sur la souveraineté étatique" (Y. POULLET, Les aspects juridiques des systèmes d'information, *Lex Electronica*, vol. 10, n°3, Hiver/Winter 2006, disponible sur le site : <http://www.lex-electronica.org/articles/v10-3/poulet.htm> et les développements consacrés tant à la montée en puissance de l'autorégulation que de la normalisation par les organisations privées ; sur ce thème, parmi de nombreux auteurs, P. TRUDEL, *Droit du cyberspace*, Ed. Thémis, Montréal, 1997, en particulier, p. 1-15 et s. ; E. KATSCH, *Law in a Digital World*, Oxford Univ. press, New York, 1995; R.H. WEBER, *Regulatory Models for the Online World*, Zurich, Schulthess (éd.), 2002, p. 80 et s.; Th. SCHULTZ, *Réguler le commerce électronique par la résolution des litiges en ligne*, Thèse dactylographiée, Genève, 2004, p. 10 à 66. ; E. LONGWORTH, Opportunité d'un cadre juridique applicable au cyberspace, in *Les dimensions internationales du droit du cyberspace*, Ed. UNESCO, Economica, Paris, 2000, p. 13 et s.).

²⁴ Ainsi, la fameuse déclaration d'indépendance de l'Internet (*Declaration of the Independence of Cyberspace*) de J.P. BARLOW : "Governments of the Industrial World . . . You have no sovereignty where we gather. . . . I declare the global social space we are building to be naturally independent of the tyrannies you seek to impose on us. . . . Cyberspace does not lie within your borders. Do not think that you can build it . . . It is an act of nature." (JP Barlow 'A Declaration of the Independence of Cyberspace' (1996) <www.eff.org/~barlow/Declaration-Final.html>)

²⁵ Pour une description de ces mesures, lire le rapport de PH. CHANTEPIE, *Mesures techniques de protection des oeuvres et DRMS, Un état des lieux*, Rapport n° 2003-02 au Ministère de la Culture, Paris, janvier 2003. Sur ces systèmes, J. COHEN, "Information Rights and Intellectual Freedom", in *Ethics and the Internet*, Aug. Vedder (ed.), Antwerpen, Interscientia, 2001, p. 20 et s. Cf. également la thèse de S. DUSOLLIER, *La protection appropriée des mesures techniques en droit d'auteur*, Larcier, Bruxelles, 2005.

²⁶ A cet égard, le point 25 de la Recommandation déjà citée de l'UNESCO sur la promotion et l'usage du multilinguisme et l'accès universel au cyberspace : « *Les Etats membres et les organisations internationales devraient accorder une grande attention à l'évolution des innovations technologiques et aux mesures de protection techniques et à leur impact sur la société de l'information dans le cadre des limitations et exceptions convenues d'un commun accord en matière de protection des droits d'auteur et des droits voisins prévues dans les traités et accords internationaux.* » + public service value

²⁷ Le SMSI, en particulier l'agenda de Tunis, charge l'UNESCO de cette réflexion sur les valeurs éthiques.

²⁸ Voir Francesco FRANCONI, Tullio SCOVAZZI (eds), *Biotechnology and International Law*, Oxford, Hart, 2006; Francesco FRANCONI (ed.), *Biotechnologies and International Human Rights*, Hart Publishing, Oxford and Portland, 2007, *Studies in International Law*, 13.

²⁹ Voir la Déclaration universelle sur la bioéthique et les droits de l'Homme, 19 octobre 2005 déjà citée.

³⁰ Cf à ce propos les travaux de Beauchamp, TL, & Childress, J.F., *Principles of Biomedical Ethics*, 3rd edn, Oxford University Press, New York, 2001.

³¹ Lire, en particulier, Jacob, F (1973) 'Le modèle linguistique en biologie', *Critique*, 322: 195-205 ; Monod, J (1970) *Le Hasard et la Nécessité. Essai sur la philosophie naturelle de la biologie moderne*, Seuil ; Morin, E. (1973) *Le paradigme perdu. La nature humaine*, Seuil. Pour une critique du modèle linguistique en biologie, voir, A. ROUVROY, *Human Genes and Neoliberal Governance. A Foucauldian Critique*, Routledge-Cavendish, 2007 (Chapter II- Scientific and Economic Strengths of Genetic Reductionism).

³² "Dignity should not be reduced to autonomy. It says more. Although originally a virtue of outstanding persons and a virtue of selfcontrol in healthy life - qualities which can be lost, for instance by lack of responsibility or in extreme illness - it has been universalised as a quality of the person as such. It now refers to both the intrinsic value of the individual and the intersubjective value of every human being in its encounter with the other. Thus it expresses the outstanding position of the human individual in the universe as being capable of both autonomy in rational action and involvement in a good life for and with the other in just institutions. Respect for the dignity of human being is respect for its inviolability in common life. Dignity concerns both oneself and the other: I must behave with dignity, and I must consider the dignity of the other; I must not give up civilised and responsible behaviour, and the other should not be commercialised and enslaved. Human rights are built on this principle of dignity."

³³ "Autonomy should not only be interpreted in the liberal sense of "permission" given for treatment and/or experimentation, instead five aspects of autonomy should be put forward: 1) the capacity of creation of ideas and goals for life, 2) the capacity of moral insight, "self-legislation" and privacy, 3) the capacity of rational decision and action without coercion, 4) the capacity of political involvement and personal responsibility, 5) the capacity of informed consent. But autonomy cannot express the full meaning of respect for and protection of the human being. Autonomy remains merely an ideal, because of the structural limitations given to it by human weakness and dependence on biological, material and social conditions, lack of information for reasoning etc. We must recognise the human person as a situated living body. A number of human individuals such as minors, coma patients and mentally ill persons cannot be considered having autonomy." (Ph. GOUJON)

³⁴ Selon l'expression de M.T. MEULDERS KLEIN, "L'irrésistible ascension de la « vie privée » au sein des droits de l'Homme", in F.SUDRE (ed.), *Le droit au respect de la vie privée au sens de la Convention européenne des droits de l'Homme*, Collection Droit et Justice 63, Bruxelles, Nemesis, Bruylant, 2005. A noter également, la distinction opérée par le Tribunal constitutionnel allemand lors de sa décision relative au recensement : "The right to self-development is not conceived as the liberty held in isolation by an individual living secluded from the rest of society, but, on the contrary, as a right enjoyed as member of a free society. It is not a question of anarchical freedom for each individual" (Bverfg., 15 décembre 1983, *EuGRZ*, 1983, p.171 et ss.. A propos de cette décision, lire E.H. RIEDL, "New bearings in German Data Protection", *Human Rights Law Journal*, 1984, Vol. 5, n°1, pp. 67 et s. et H. BURKERT, "Le jugement du Tribunal constitutionnel fédéral allemand sur le recensement démographique et ses conséquences", *Dr. Inf.*, 1985, p. 8 et s.. Enfin, la distinction opérée par H. ARENDT entre "Liberty" et "Freedom" (H. ARENDT, *On Revolution*, Penguin Classics, 1963, p. 32 : « Liberties (...) are the result of liberation but they are by no means the actual content of freedom, which (...) is participation in public affairs, or admission to the public realm ».

³⁵ Sur ce point, l'article de N. ROULAND, "A propos des droits de l'Homme: un regard anthropologique", *Droits fondamentaux*, n° 3, Janvier- Décembre 2003, p. 129 et s. qui cite notamment la déclaration finale de Bangkok du 13 octobre 2003 (déclaration qui a précédé la Conférence mondiale des droits de l'Homme de Vienne organisée par les Nations Unies en 1993) : " Si les droits de l'Homme sont par nature universels, ils doivent être envisagés dans le contexte du processus dynamique et évolutif de fixation des normes internationales , en ayant à l'esprit l'importance des particularismes nationaux et régionaux comme des divers contextes historiques, culturels et religieux" (A/CONF. 157/24, 13 octobre 1993).

³⁶ Selon Ph. GOUJON (op.cit.) : "“Beneficence” is the expectation that the use of the system will be for doing good. “Non maleficence” is the expectation that the system will not be used with bad intent.”

« Dès 1972, la [Conférence mondiale sur l'environnement de Stockholm](#) organisée dans le cadre des [Nations Unies](#) a posé les premiers droits et devoirs dans le domaine de la préservation de l'environnement. Ainsi, le principe 1 de la **déclaration de Stockholm** énonce : « L'homme a un droit fondamental à la liberté, à l'égalité et à des conditions de vie satisfaisantes, dans un environnement dont la qualité lui permette de vivre dans la dignité et le bien-être. Il a le devoir solennel de protéger et d'améliorer l'environnement pour les générations présentes et futures ». Les prémices modernes du principe de précaution

viennent d'Allemagne, dans le courant des [années 1970](#) : *Vorsorgeprinzip* (« principe de prévoyance »). Afin d'inciter les entreprises à utiliser les meilleurs techniques disponibles, sans mettre en péril l'activité économique, ce principe incite à prendre des mesures contre les pollutions avant d'avoir des certitudes scientifiques sur les dommages causés à l'environnement. Dès les années 1984², 1987³ et suivantes, des textes officiels internationaux en font mention dans les pays d'Europe du Nord.. Mais c'est au cours du [Sommet de la Terre réuni à Rio de Janeiro en juin 1992](#) que ce principe bénéficie d'une reconnaissance planétaire (point 8 du préambule de la [convention de Rio sur la diversité biologique](#)). Dans l'histoire de la construction européenne, le principe de précaution est introduit avec le **Traité de Maastricht** (art. 130R devenu 174 avec le Traité d'Amsterdam) : « La politique de la Communauté [...] vise un niveau de protection élevé [...]. Elle est fondée sur le principe de précaution et d'action préventive, sur le principe de correction, par priorité à la source, des atteintes à l'environnement et sur le principe du pollueur - payeur ». Le principe de précaution évolue ainsi d'une conception philosophique vers une norme juridique. La Commission européenne, dans sa communication du [2 février 2000](#), sur le recours au principe de précaution, définit ainsi des lignes directrices à ce propos » (Définition Wikipedia.fr).

³⁸ L'opposition entre la vision orwellienne et celle Kafkaïenne est remarquablement décrite par l'ouvrage de D. J SOLOVE : « *The digital person- technology and privacy in the information age* », New York University Press, New York, 2004, particulièrement p. 7 et s. : « *The dominant metaphor for modern invasions of Privacy is Big Brother... Big Brother oppresses its citizens, purges, dissenters, and spies everyone in their homes. The result is a cold, drab grey world with hardly any space for love, joy, original thinking, spontaneity or creativity. It is a society under total control. Although the metaphor has proven quite useful for a number of privacy problems, it only partially captures the problems of digital dossiers. Big Brother envisions a centralized authoritarian power that aims for absolute control, but the digital dossiers constructed by business aren't controlled by a central power, and their goal is not to oppress us but to get us to buy new products and services* ».

³⁹ « *The trial captures an individual's sense of helplessness, frustration and vulnerability when a large bureaucratic organization has control over a vast dossier of details about one's life... The problem is not simply a loss of control over personal information nor is there a diabolical motive or plan for domination as with Big Brother... The problem is a bureaucratic process that is uncontrolled..* » (SOLOVE, p. 9).

⁴⁰ D.J. SOLOVE, « Privacy and Power: Computer Data Bases and Metaphors for Information Privacy », 53 *Stanford Law Review*, 2001, 6, p. 1393 et s.

⁴¹ L'importance du respect des « contextes », c'est-à-dire des zones de confiance dans lesquelles une donnée à caractère personnel est transmise par la personne concernée a été remarquablement mise en évidence par H.NISSENBAUM (« Privacy as contextual Integrity », 79 *George.Washington Law Rev.*,2004, pp. 150 et s.). L'auteur affirme: « *the freedom from scrutiny and zones of "relative insularity" are necessary conditions for formulating goals, values, conceptions of self, and principles of action because they provide venues in which people are free to experiment, act and decide without giving account to others or being fearful of retribution* ».

⁴² Les dangers de l'opacité de nos sociétés de l'information comme menace pour nos sociétés de l'information, où les citoyens ne peuvent connaître de manière exacte le fonctionnement des systèmes d'information, les données collectées, les lieux de traitement, les finalités poursuivies par ceux qui traitent les données, sont mis en évidence dès 1983 par le fameux jugement constitutionnel dans l'affaire du recensement (Bundesverfassungsgerichtshof, 15 Décembre 1983, *EuGRZ*, 1983,p.171 et s.). La tentation des citoyens est alors d'adopter le comportement qu'ils croient attendu par la société et de ne point oser s'exprimer librement, ce qui est dommageable pour nos démocraties : « *The possibility of inspection and of gaining influence have increased to a degree hitherto unknown, and may influence the individuals' behaviour by the psychological pressure exerted by public interests. Even under certain conditions of modern information processing technology, individual self-determination presupposes that the individuals left with the freedom of decision about actions to be taken or to be omitted, including the possibility to follow that decision in practice. If someone cannot predict with sufficient certainty which information about himself in certain areas is known to his social milieu and cannot estimate sufficiently the knowledge of parties to whom communication may be possibly be made, he is crucially inhibited in his freedom to plan or to decide freely and without being subject to any pressure influence. If someone is uncertain whether deviant behaviour is noted down and stored permanent as information, or is applied or passed, he will try not to attract attention by such behaviour. If he reckons that participation in an assembly or a citizens' initiative will be registered officially and that personal risks might result from it, he may possibly renounce the exercise of his respective rights. **This would not only impact his***

chances of development but would have also impact the common good (“Gemeinwohl”), because self-determination is an elementary functional condition of a free democratic society based on its citizen’s capacity to act and to cooperate.”

⁴³ Ce danger de « réductionnisme » est déjà dénoncé en 1966 par KARST (« « The files » : Legal Control Over the Accuracy and Accessibility of Stored Personal Data », 31 *Law and Contemporary problems*, 1966, p. 361) qui souligne le danger d’ « a centralized, standardized data processing » qui ne retient comme signifiants, à propos du sujet de la recherche, que les faits repris et traités par l’ordinateur. Dans le même sens, l’ouvrage de J. ROSEN, *The unwanted Gaze : the Destruction of Privacy in America*, 2000, cité par D.J. SOLOVE, *ibidem*, p. 424 : « *Privacy protects us from being midedined and judged out of context in a world of short attention spans, a world in which information can easily be confused with knowledge* ».

⁴⁴ C’est précisément la raison de l’article 15 de la directive européenne 95/46 en matière de protection des données qui prévoit des dispositions en matière de systèmes automatisés de décision. La préoccupation majeure a trait à l’automatisation croissante des processus décisionnels à l’égard des individus. Comme le révèlent les travaux préparatoires, le législateur européen en est venu à s’inquiéter d’une telle automatisation tant elle diminue le rôle joué par les personnes dans les processus de décision: « *This provision is designed to protect interest of the data subject in participating in the making of decisions which are of importance to him. The use of extensive data profiles of individuals by powerful public and private institution deprives the individual the capacity to influence decision-making processes within those institutions, should decisions be taken on the sole basis of his ‘data shadow’* ». Une autre préoccupation concerne le fait que l’automatisation galopante des processus de décision engendre une acceptation quasi-automatique de la validité et de la pertinence de ces décisions et, corrélativement, un désinvestissement et une déresponsabilisation de décideurs « humains ». A cet égard, la Commission relève que « *the results produced by the machine, using more and more sophisticated software, and even expert system, has an apparently objective and incontrovertible character to which a human decision-maker may attach too much weight, thus abdicating his own responsibilities* »

⁴⁵ Sur cette distinction classique et sa radicale remise en cause, J.A. FICHBAUM, « Towards an autonomy-based theory of constitutional Privacy : Beyond the ideology of familial privacy », *Harvard Civil Rights –Civil Liberties Review*, 1979, 14, 361-384. Sur ce point lire également, D.J. SOLOVE, « Conceptualizing Privacy », 90 *California Law Review*, 2002, spécialement p. 1138 et 1139.

⁴⁶ Bundesverfassungsgericht, 15 décembre 1983, *EuGRZ*, 1983, p.171 et s. déjà cité note 41. Sur cette décision, lire E.H. RIEDL, “New bearings in German Data Protection”, *Human Rights Law Journal*, 1984, Vol. 5, n°1, p. 67 et s.; H. BURKERT, “ Le jugement du Tribunal constitutionnel fédéral allemand sur le recensement démographique et ses conséquences”, *Dr. Inf.*, 1985, p. 8 et s..

⁴⁷ Voir D. LYON, « An electronic Panopticon ? A sociological critique of the surveillance society », *Sociological Review*, 1993, 41(4), 653-678. Pour une analyse de ces enjeux, voir A. ROUVROY, "Privacy, Data Protection, and the Unprecedented Challenges of Ambient Inteligence" (September 11, 2007). Available at SSRN: <http://ssrn.com/abstract=1013984>

⁴⁸ Cf note 41

⁴⁹ Cf. en particulier le point 53 de la déclaration de Tunis : « *Nous prenons l’engagement d’œuvrer résolument en faveur du multilinguisme de l’Internet ... Dans ce cadre, nous prônonons en outre l’utilisation des langues locales pour l’élaboration des contenus, la traduction et l’adaptation, les archives numériques et les diverses formes de médias numériques et électroniques et nous sommes conscients que ces activités peuvent également renforcer les communautés locales et autochtones. De ce fait, nous souhaitons insister sur la nécessité : a) de faire progresser l’adoption du multilinguisme dans un certain nombre de secteurs : noms de domaine, adresses de courrier électronique, recherche par mots-clé ; de mettre en œuvre des programmes autorisant la présence de noms de domaine et de contenus multilingues sur l’Internet et d’utiliser divers modèles de logiciel pour faire face au problème de la fracture numérique linguistique et assurer la participation de tous dans la nouvelle société qui se fait jour ; c)...* ».

⁵⁰ Convention sur la protection et la promotion de la diversité des expressions culturelles, adoptée par l’assemblée générale de l’UNESCO, Paris, le 20 octobre 2005.

⁵¹ Le *data mining* (littéralement : « forage de données », plus significativement « extraction de la connaissance » ou « exploitation stratégique des données ») peut se définir comme « l'application des techniques de statistiques, d'analyse de données et d'intelligence artificielle à l'exploration et à l'analyse sans *a priori* de (souvent grandes) bases de données informatiques, en vue d'extraire des informations nouvelles et utiles pour le détenteur de ces données »⁵¹. Cette notion recouvre donc l'ensemble des nouvelles techniques et méthodes qui ont pour but d'explorer et d'amener à la surface de manière exhaustive des relations à partir d'une masse importante de données pouvant relever de sources et de bases de données diverses (S. TUFFERY, *Data mining et statistique décisionnelle. L'intelligence dans les bases de données*, Ed. Technip, Paris, 2005, p. VII.)

⁵² Pour L. A. Bygrave, le profilage peut être défini de la manière suivante : « *Generally speaking, profiling is the process of inferring a set of characteristics (typically behavioural) about an individual person or collective entity and then treating that person/entity (or other persons/entities) in the light of these characteristics. As such, the profiling process has two main components : (i) profile generation – the process of inferring a profile ; (ii) profile application – the process of treating persons/entities in light of this profile* » (L. A. BYGRAVE, « Minding the machine : Article 15 of the EC Data Protection Directive and Automated Profiling », *Computer Law & Security Report*, 2001, vol. 17, pp. 17-24, disponible en ligne à l'adresse <http://www.austlii.edu.au/au/journals/PLPR/2000/40.html>).

⁵³ « *Certains chercheurs du MIT s'emploient à développer des logiciels sophistiqués (recommendations systems) qui ne se limitent pas à un seul domaine d'application et à certaines données spécifiques, comme ceux utilisés dans le cadre de sites de commerce électronique tels qu'Amazon ou eBay. L'objectif visé par ces recherches est de ne pas se restreindre aux données propres à l'utilisateur, envisagé dans le contexte d'une application unique et déterminée mais de privilégier le profilage de la personne dans son ensemble : « we must start modeling the person, rather than the user ». Qualifiée de « social data mining », la technique est destinée à construire des profils plus riches, notamment en analysant les données collectées sur des sites de « réseautage virtuel » (web-based social networks) qui fleurissent ces derniers temps sur Internet tels que Friendster, MySpace ou Facebook. Ces plates-formes numériques en vogue se révèlent des sources précieuses d'informations sur les individus et les communautés socioculturelles dans lesquelles ils s'inscrivent. En effet, les individus ne font pas seulement qu'y mentionner leurs amis et connaissances, ils s'y décrivent eux-mêmes et tiennent également à jour un inventaire détaillé de leurs activités, de leurs intérêts et de leurs passions (littérature, musique, télévision, spectacles, films, sports, nourriture, etc.)* » (Jean-Marc Dinant, Christophe Lazaro, Yves Pouillet, Nathalie Lefever, Antoinette Rouvroy, L'application de la Convention 108 au mécanisme de profilage - Eléments de réflexion destinés au travail futur du Comité consultatif (T-PD), étude à paraître).

⁵⁴ Pour de nombreux exemples, lire PH. LEMOINE, « Commerce électronique, marketing et liberté », in Groupe d'études Société d'information et vie privée (P. Tabatoni sous dir. de), *La protection de la vie privée dans la société d'information*, t. II, 2000, disponible en ligne à l'adresse <http://www.asmp.fr/travaux/gpw/internetvieprivée/rapport2/chapitr7.pdf>.

⁵⁵ Cf. sur ce point les réflexions de L. LESSIG, *The future of ideas*, New York Random House, 2001. Voir aussi, D.L. BURK et J.E. COHEN, « Fair use Infrastructure for Rights Management Systems », 15 *Harvard Journal of Technology and Law*, 2001, p. 41 et s.

⁵⁶ Sur cette notion de « digital divide » à facettes multiples et la politique d'accès universel, lire les points 10, et s. de la Déclaration de principe de Tunis qui évoque les multiples fractures engendrées par le développement de la société de l'information entre femmes et hommes, territoires isolés et agglomérations urbaines, pays pauvres et riches, jeunes et personnes âgées, etc. La politique d'accès universel évoque au-delà de l'accès à l'infrastructure, la connexion de lieux publics (enseignement, santé et bibliothèque), l'accès à l'information et au savoir et le développement d'un domaine public informationnel fort).

⁵⁷ Nous nous référons à l'ouvrage désormais classique de Lessig, *Code and other laws of Cyberspace*, New York, Basic Books, 1999.

⁵⁸ Cf. parmi de nombreux auteurs, les auteurs cités note 51.

⁵⁹ Voir sur ce point l'avis du Groupe européen d'Ethique des sciences et des nouvelles technologies auprès de la Commission européenne, Aspects éthiques des implants TIC dans le corps humain, 16 mars 2005.

⁶⁰ Sur ce point, les réflexions de P. SCHWARTZ, (« *Beyond Code for Internet Privacy : Cyberspace Filters, Privacy control, and Fair Information Practice* », *Wisconsin Law Rev.*, 2000, p.787.) : « *In place of Lessig's idea that privacy protects a right of individual control, this Article has developed a concept of constitutive privacy. Information Privacy is a constitutive value that safeguards participation and association in a free society. Rather than simply seeking to allow more and more individual control of personal data, we should view the normative function of information privacy as inhering in its relation to participatory democracy and individual self determination. Information Privacy rules should carry out a constitutive function by normally defining multidimensional information territories that insulate personal data from the observation of different parties.* ». Cf. également, P.DE HERT and S.GUTWIRTH ("Privacy, Data Protection and law enforcement. Opacity of the individuals and Transparency of the power", in *Privacy and the Criminal Law*, E.CLAES et alii (ed.), Intersentia, Antwerpen-Oxford, 2006, p.74): "Never does an individual have an absolute control over an aspect of his or her privacy. If individuals do have freedom to organise life as they please, this will only remain self-evident up to the point that it causes social or inter-subjective friction. At that stage, the rights, freedoms and interests of others, as well as the prerogatives of the authorities come into play. The friction, tension areas and conflicts create the need for a careful balancing of the rights and interests that give privacy its meaning and relevance. That shows clearly, although quintessential for a democratic constitutional state, because it refers to liberty, privacy is a relational, contextual and per se social notion which only requires substance when it clashes with other private or public interests." Sur ce point, lire aussi, Y. POULLET et A. ROUVROY, " Privacy or self-determination as the key concept", in *Reinventing Data Protection, Proceedings of the Brussels Colloquium 14-15 novembre 2007*, Springer Verlag, 2008, à paraître.

⁶¹ H. BURKERT, Dualities of Privacy -An Introduction to "Personal Data Protection and Fundamental Rights", in " Data Protection – Emerging issues", M.V. PEREZ, P. PALAZZI, Y. POULLET, Cahiers du Crid, n° 31, Bruylant, Bruxelles, 2008, à paraître.

⁶² Sur ce point F. RIGAUX, *La vie privée, une liberté parmi les autres ?*, Bruxelles, Bruylant, 1990, spécialement p.724 et s. et surtout D. SOLOVE, « Conceptualizing Privacy », article déjà cité, p. 1127 où l'auteur prône une approche pragmatique : « *My approach to conceptualizing Privacy draws from a few recurring ideas of pragmatism : a recognition of context and contingency, a rejection of a priori knowledge and a focus on concrete practices.* »

⁶³ « *La « privacy » serait ici simplement ce que l'individu fait de la liberté qui lui est reconnue. Elle n'est pas définissable a priori : sa portée n'apparaît qu'à travers les conflits que suscite son exercice, c'est-à-dire qu'elle n'est appréhendée par le droit que dans un cadre contextualisé* » (C'est par ces mots que de SCHUTTER (*La vie privée entre droit de la personnalité et vie privée* », *Rev. trim. dr. h.*, 1999, p.861) résume la position de RIGAUX, (« *La vie privée. Une liberté parmi les autres !* », *Travaux de la faculté de droit de Namur*, Bruxelles, Larcier, 1992, p. 120 et s.).

⁶⁴ Sur ce droit à la séclusion à l'origine du concept de privacy, J.D. SOLOVE, "Conceptualizing Privacy", 90 *California Law Rev.*, 2001, pp. 1041-1043. Sur l'importance de cet aspect de la privacy comme condition de structuration de l'individu, lire J. RAYMAN, "Driving to the Panopticon: A Philosophical Exploration of the Risks to Privacy Posed by the Highway of the Future", 11 *Santa Clara Computer & Techn. Law Journal*, 1995, pp. 22 et s.; J. COHEN, "Examined Lives: Informational Privacy and the Subject as Object", 52 *Stanford Law Rev.*, 2000, pp. 1373 et s. et surtout H.NISSENBAUM, "Privacy as contextual Integrity", 79 *George.Washington Law Rev.*, 2004, p. 150 qui note : "the freedom from scrutiny and zones of "relative insularity" are necessary conditions for formulating goals, values, conceptions of self, and principles of action because they provide venues in which people are free to experiment, act and decide without giving account to others or being fearful of retribution".

⁶⁵ On cite volontiers à ce propos deux arrêts de la Cour européenne des droits de l'Homme : l'affaire Guerra jugée en 1998 et surtout celle Moreno Gomez (Arrêt du 16 novembre 2004) cette fois à propos d'industries polluantes. Sur ces affaires, J.P. MARGUENAUD, « *De l'identité à l'épanouissement* », in *Le droit au respect de la vie privée au sens de la Convention européenne des droits de l'Homme*, déjà cité, p. 220 et s.

⁶⁶ Sur ces extensions progressives, lire les conclusions de M. T. MEULDERS-KLEIN, « *L'irrésistible ascension de la "vie privée" au sein des droits de l'Homme* », in *Le droit au respect de la vie privée au sens de la Convention européenne des droits de l'Homme*, op.cit., p. 308. et les références à nombre d'auteurs, On renverra le lecteur en particulier à l'ouvrage majeur de F.RIGAUX, *La protection de la vie privée et des autres biens de la personnalité*, Bruylant, Bruxelles, 1990. Voir également à cet égard, S.GUTWIRTH, « *Privacyvrijheid ! De vrijheid om zichzelf te zijn* », Rathenau Instituut, Den Haag, Juin 1998, p. 51 et s.

⁶⁷ Sur ce droit, né des obligations positives de l'Etat dans une société contemporaine dite de l'information, lire la thèse de C.DE TERWANGNE, *Société de l'information et mission publique d'information*, Thèse dactylographiée, Namur, 1999-2000.

⁶⁸ Sur les obligations positives de l'Etat, lire entre autres, F.SUDRE, « Rapport introductif », in F.SUDRE (ed.), *Le droit au respect de la vie privée au sens de la Convention européenne des droits de l'Homme*, Bruxelles, Bruylant, Némésis, 2005, p. 7 et s..

⁶⁹ Sur cette « horizontalisation » des droits de l'Homme et en particulier de la vie privée, lire S. VANDROOGHENBOECK, « L'horizontalisation des droits de l'homme », in H.DUMONT et alii (ed.), *La responsabilité, face cachée des droits de l'Homme*, Bruxelles, Bruylant, 2005, p. 355 à 390.

⁷⁰ Sur cet équilibre entre droits, libertés et intérêts, lire Y. POULLET, « La protection des données, entre libertés, droits subjectifs et intérêts légitimes », in *Liber amicorum P. Martens*, Bruxelles, Larcier, 2007, p. 133 à 150. Sur la méthode de pondération des intérêts comme seule méthode permettant de définir, dans le concret, les contours de la vie privée, lire F. RIGAUX, *op.cit.*, p. 750 : « *Le concept juridique de vie privée ne saurait donner lieu à une application syllogistique permettant d'identifier par une opération purement logique la situation appréhendée par le concept de vie privée. La méthode de pondération d'intérêts est la seule appropriée mais comme son terme l'indique, loin de se prononcer sur l'étendue d'un droit subjectif, le juge pèse les intérêts respectifs des parties en présence à la lumière de l'intérêt général* ».

⁷¹ Rapport explicatif de la Convention n° 108.

⁷² C'est à ces deux valeurs, fondement de la Constitution allemande que se réfère le Tribunal constitutionnel allemand dans l'affaire du recensement déjà citée : *“The standard to be applied is the general right to the free development of one's personality. The value and dignity of the person based on free self-determination as a member of the society is the focal point of the order established by the Basic Law (Grundgesetz). The general personality right as laid down in Art. 2 (1) and Art. 1 (2) GG serves to protect these values – apart from other more specific guarantees of freedom- and gains in importance if one bears in mind modern developments with attendant dangers to the Human personality.”*

⁷³ Cf. les écrits de LESSIG déjà cités. Selon cet auteur, il est important dans la reconnaissance de la « privacy » de tenir compte de l'architecture du système dans lequel la préoccupation de la défense de celle-ci doit intervenir et de l'évolution de cette architecture.

⁷⁴ J.R. REIDENBERG, *“Lex informatica” : the formulation of Information Policy Rules through Technology.*, 76 *Texas Law Review*, 1998, p. 553 et s.; du même auteur, *“Governing Networks and Rule-Making in Cyberspace”*, 45 *Emory Law Journal*, 1996, p. 911 et s.

⁷⁵ Sur le droit à l'anonymat ainsi que sur les nouveaux principes qu'impose la prise en considération du progrès technologique, lire nos réflexions in : « La protection des données, un nouveau droit constitutionnel? Pour une troisième génération de réglementations de protection des données », *Recueil des cours de l'Académie internationale de droit constitutionnel de Tunis*, Session de 2007, Tunis (à paraître) : « Les caractéristiques de l'environnement des services de communication électronique (omniprésence, complexité, opacité, performance et polyvalence) et des terminaux (interactivité, dimension internationale, opacité de fonctionnement) créent de nouveaux risques et aggravent les risques d'atteinte aux libertés individuelles et à la dignité humaine. La parade à ces risques n'est possible que par la consécration de principes nouveaux améliorant la protection des individus et lui donnant une meilleure maîtrise de leur environnement. Ce n'est en effet que dans la mesure où cette maîtrise est possible, que la personne concernée pourra prendre effectivement la responsabilité de sa propre protection et mieux disposer des moyens d'une véritable autodétermination informationnelle ».

⁷⁶ A ce propos, F. BLANCHETTE, « L'expectative raisonnable de vie privée et les principaux contextes de communication électronique dans Internet », 2004 *Juriscomnet* disponible en ligne : <http://juriscom.agat.net/uni/visu.php?ID=425>

⁷⁷ A notre sens, l'autodétermination n'est pas à proprement parler un droit, c'est bien plutôt une capacité qui doit être respectée par le droit lorsqu'elle trouve à s'exprimer, et une capacité dont le droit doit favoriser le développement et l'expression le cas échéant.

⁷⁸ Comme le note déjà la Cour constitutionnelle allemande dans l'arrêt du recensement précité : «The individuals does not possess a right in a sense of an absolute, unlimitable mastery of "his" data; rather he is a personality dependant on communication developing within the social community. Information, even if personality based, is a reflection of social reality and cannot be associated purely with the individual concerned. The Basic Law has decided the tension between the individual and society in favour of the individual being community related and community bound".

⁷⁹ A propos des PICS, outre l'opinion émise par le Groupe de l'article 29 (Opinion 11/98 du Groupe européen de protection des données, Groupe dit de l'article 29 à propos de la Platform for Privacy Preferences (P3P) et des Open Profiling Standards (OPS), opinion disponible à http://europa.eu.int/comm/dg15/fr/media/dataprot/wpdocs/wp11_fr.pdf), lire sur ce protocole, J. CATLETT, « Technical Standards and Privacy : An open Letter to P3P Developers », disponible à l'adresse : <http://www.junkblusters.com/standards.html>. Sur la contractualisation du traitement des données ainsi opérée par la technologie, lire P.M. SCHWARTZ, « Beyond Lessig's Code for Internet Privacy : Cyberspace, Filters, Privacy control and Fair Information Practices », *Wisconsin Law Review*, 2000, p. 749 et s. ; M. ROTENBERG, « What Larry doesn't Get the Truth », *Stan. Techn. L. Rev.*, 2001,1, disponible sur le site : http://www.sth.Stanford.edu/STLR/Articles/01_STLR_1.

⁸⁰ Voir Amartya Sen, *Inequality Reexamined*, Harvard University Press, 1995.

⁸¹ Margaret Jane Radin, "Justice and the Market Domain", in John Chapman, J. Roland Pennock, *Markets and Justice*, New York University Press, 1989, p. 168. : " the domino theory asserts that market evaluations of objects and activities are imperialistic, diving out other and better ways of perceiving and evaluating objects and activities. Once some individuals attach a price at a given object, relation or activity, they and others tend to lose their capacity to perceive or evaluate that object, relation or activity as anything but a commodity with a specific market price. Moreover, the theory asserts, once certain objects or activities are commodified, there is a tendency for other objects or activities of the same sort or even of other sorts also to be seen and evaluated merely in terms of their actual or potential market value." Pour une exploration plus détaillée de ce thème voir Antoinette Rouvroy, "Information génétique et assurance. Discussion critique autour de la position « prohibitionniste » du législateur belge », *J.T.*, n°5978, 2000, 585-603 et Antoinette Rouvroy, *Human Genes and Neoliberal Governance : A Foucauldian Critique*, Routledge-Cavendish, 2007, (Chapter 7 : A critical assessment of economic and actuarial perspectives on genetics and insurance)

⁸² H. Nissenbaum, "Privacy as Contextual Integrity" *Washington Law Review*, vol. 79, n.1, February 04, 2004. 119-158.

⁸³ Comité des Ministres, Déclaration sur la liberté de communication sur l'Internet, 840^{ème} session, 28 mai 2003, disponible sur le site du Conseil de l'Europe (<http://www.coe.int>)

⁸⁴ A cet égard, la déclaration citée note précédente qui se réfère à la Recommandation du Conseil des ministres du Conseil de l'Europe, n°R (99) 14 relative au service universel relatif aux nouveaux services de communication et d'information.

⁸⁵ Pour une comparaison entre la jurisprudence européenne fondée sur l'article 10 de la CEDH et celle américaine fondée sur le premier amendement de la Constitution américaine, lire P.Y. DOCQUIR, Variables et variations de la liberté d'expression en Europe et aux Etats Unis, Coll. Droit et Justice, n° 72, Bruylant-Nemesis, Bruxelles, 2007.

⁸⁶ Sur ce point, lire Unité d'évaluation des choix scientifiques et techniques de la direction générale des études du Parlement européen, *Technologies de sécurité pour les médias digitaux- Rapport final*, Bruxelles, Direction générale des études du parlement européen, mai 2001, p. 39 , disponible en ligne : http://www.europarl.eu.int/STOA/publi/pdf/00-06-01_fr.pdf. Lire également parmi de nombreux auteurs, E.G. CARLISLE, « Copyright Management Systems - Accessing the power balance », in *The Information Society*, C. ZIELINSKI and alii (eds), Proceedings of the IFIP Conference, Turku, June 27-29, 2005, Springer, p. 211 et s. ; J. COHEN, « DRM and Privacy », 18 *Berkeley Technology Law Journal*, 2003, 575

⁸⁷ Sur ces mouvements, lire C. DIBONA, S. OCKMAN et M. STONE (eds), *Open Source : Voices from the open Source Revolution*, O'Reilly and Assoc., 1999

⁸⁸ « *La diversité culturelle est le patrimoine commun de l'humanité. La société de l'information devrait être fondée sur le respect de l'identité culturelle, de la diversité culturelle et linguistique, des traditions et des religions, devrait promouvoir ce respect et favoriser le dialogue entre les cultures et les civilisations. La promotion, l'affirmation et la préservation des différences culturelles, objets de documents pertinents approuvés par les Nations Unies et notamment par la Déclaration universelle de l'UNESCO sur la diversité culturelle, enrichiront davantage la société de l'information* » (SMSI, Déclaration de principe, Construire la Société de l'Information : un défi mondial pour le nouveau millénaire, Genève, 12 décembre 2003).

⁸⁹ Convention du Conseil de l'Europe sur la cybercriminalité du 23 novembre 2001 (STE, n° 185).

⁹⁰ Y compris dans l'Union européenne, où la directive du 14 mars 2006 sur la rétention des données de trafic (JO, 15 mars 2006, L 105, p. 54 et s.) oblige les fournisseurs de services de communication à « retenir » les données de trafic pendant une durée minimale de six mois pour les données de trafic relatives à des services Internet et de douze mois dans le cas de données relatives à des services téléphoniques. Sur cette directive, lire E. KOSTA et P. VAELCKE, Retaining the Data Retention Directive, *CL&SR*, 2006, p. 370 et s.).

⁹¹ Ainsi, les ayants droit des titulaires de droit de propriété intellectuelle réclament la possibilité d'investigations propres pour lutter contre les copies illicites. A cet égard, l'actuel procès pendant devant la Cour européenne de Justice.

⁹² Sur ce point, lire P.DE HERT et S.GUTWIRTH, "Privacy, Data Protection and law enforcement. Opacity of the individuals and Transparency of the power", in *Privacy and the Criminal Law*, E.CLAES et alii (ed.), Intersentia, Antwerpen-Oxford, 2006, p.74.

⁹³ Sur ces diverses facettes de l'accès universel présentes dans la Déclaration de principes du SMSI de Genève, supra nos remarques, note 55.

⁹⁴ On souligne que le Conseil de l'Europe considère que le droit d'accès aux documents du secteur public se justifie par le fait qu'une personne ne peut être considérée comme libre de s'exprimer que si elle dispose des éléments nécessaires à la compréhension de l'environnement sociétal dans lequel elle évolue.

⁹⁵ Pour un vaste "domaine public informationnel" et sa promotion par l'UNESCO, lire le point 15 de "Recommendation concerning the Promotion and Use of Multilingualism and Universal Access to Cyberspace", adopted by the UNESCO General Conference at its 32nd session (Oct. 2003) : "Member States should recognize and enact the right of universal online access to public and government-held records including information relevant for citizens in a modern democratic society, giving due account to confidentiality, privacy and national security concerns, as well as to intellectual property rights to the extent that they apply to the use of such information. International organizations should recognize and promulgate the right for each State to have access to essential data relating to its social or economic situation."

⁹⁶ A cet égard, les conclusions de la Smart Card Alliance du 3 novembre 2006 (disponible sur le site : <http://www.smartcardalliance.org/pages/publications-whti-passport-card>) à propos de l'utilisation de la technologie RFID dans les passeports et la possibilité de lire à distance ceux-ci : « *the vicinity read Rfid Technology proposed for the passport card, in combination with its weak cryptographic protection, will feed citizen distrust due to the undeniable observation by some technologies that the citizen's unique reference number could be obtained and used to track the citizen whenever the card is outside of its protective sleeve. This raises serious privacy concerns that will have to be overcome if the program is to be embraced by Americans* ». Dans le même sens, la Déclaration de Budapest sur les documents de voyage à lecture automatique (MRTD-Machine Readable Travel Documents) disponible sur le site de la FIDIS (projet de recherche européen) : <http://www.fidis.net/press-events/press-releases/declaration-de-budapest>.

⁹⁷ Sur ces diverses relations entre Droit et Technologie, Y. POULLET, « Technology and the Law : From Challenge to Alliance », in U. GASSER (ed.), *Information Quality Regulation: Foundation, Perspectives and applications*, Zurich, Schulthess, 2004, p. 25 et s. et la thèse d'E. LABBE, *Les équilibres juridiques à l'épreuve de la contrainte technique – Conflits et défis normatifs de la société de l'information*, Thèse dactylographiée, Université de Montréal, 2006.

⁹⁸ Ainsi, les « Privacy Enhancing Technologies » (PETs), les « Consumer Protection Enhancing Technologies » (CEPTs), les « Intellectual Protection Enhancing Technologies » (IPETs). A propos de ces technologies apportant une plus-value à l'effectivité des solutions légales et, de manière plus générale, sur les relations entre Droit et Technologie, lire nos réflexions in *Mélanges G. HORSMANS*, Bruylant, 2004, p. 942 et s. récemment, lire la recommandation de la Commission européenne prônant le recours aux PETs.

⁹⁹ On ajoutera la disposition de l'article 5.3 de la directive 2002/58 CE dite « Protection des données et secteur des communications électroniques », qui interdit de pénétrer dans le terminal sans le consentement de l'utilisateur ». Sur cette directive et cette disposition en particulier, lire le commentaire de K. ROSIER, xxxx

¹⁰⁰ En particulier, l'article 16 de la Directive 95/47 CE qui oblige le responsable du traitement de données à caractère personnel à prendre des mesures techniques et organisationnelles appropriées eu égard à l'état de la technologie, aux coûts des mesures envisageables et aux risques d'atteinte à la confidentialité.

¹⁰¹ C. CLARK, « The answer to the Machine is in the Machine », in B. HUGENHOLTZ (ed.), *The future of Copyright a digital environment*, La Haye, Kluwer Law Int., 1996, p. 139.

¹⁰² Non seulement publiques comme l'ISO, le CEN, l'ETSI mais également privées comme le W3C, l'IETF ou le GS 1 en matière de RFID.

¹⁰³ Sur le principe de précaution et le devoir tant de vigilance que d'évaluation des risques, lire A. STIRLING, *On science and precaution in the management of technological risk*, a ESTO project report, prepared for the European Commission – JRC- Institute Prospective Technological Studies, May 1999, EUR 19056 EN (a synthesis report of studies conducted by Renn O., Klinke A., Rip A., Salo A., Stirling A.). Cf. également Conseil fédéral du développement durable, *Avis sur la communication de la Commission européenne sur le recours au principe de précaution (COM(2000) 1)*, approuvé par l'A.G. du 17 octobre 2000, p.11, d'après STIRLING Andrew, « Sciences et risques : aspects théoriques et pratiques d'une approche de précaution » in ZACCAÏ E. et MISSA J.N.(eds.), *Le principe de précaution, significations et conséquences*, Ed.ULB, 2000..

¹⁰⁴ Sur les principes de l'économie et du droit de l'environnement, lire O. GODARD, C. HENRY, P. LAGADEC, E. MICHEL-KERJAN, *Traité des nouveaux risques - Précaution, Crise, Assurance*, Gallimard, Folio actuel, Paris, 2002.

¹⁰⁵ La Convention sur l'accès à l'information, la participation du public au processus décisionnel et l'accès à la justice en matière d'environnement, dite Convention d'Aarhus, a été signée lors de la quatrième Conférence ministérielle «Un environnement pour l'Europe» à Aarhus (Danemark) le 25 juin 1998. Cette Convention a été rédigée dans le cadre de la Commission économique pour l'Europe des Nations-Unies (CEE-ONU), en application du Principe 10 de la Déclaration de Rio (1992). Le texte final de la Convention est le résultat de plusieurs années de négociations entre les gouvernements et la société civile représentée par une coalition d'ONG. Ses dispositions vont bien au-delà des règles qui existent en matière d'environnement dans le droit international et dans de nombreuses législations nationales. La Convention d'Aarhus est entrée en vigueur en octobre 2001 après le nombre nécessaire de ratifications.