Les droits de l'homme numérique

Jean-François Henrotte

Avocat (Lexing), collaborateur scientifique (Ulg) et directeur de la Revue du droit des technologies de l'information *Esra Tosun* – Bruxelles, Belgique

La révolution numérique a bouleversé les habitudes de tous, allant du simple citoyen aux autorités publiques. La vente de produits nazis interdits à la vente en France *via* le site Web Yahoo [1] ou encore la comparaison sur les réseaux sociaux de l'ancienne Ministre de la Justice, Christiane Taubira, à un singe [2] illustrent les difficultés croissantes liées à l'utilisation de l'Internet. Si cet outil renforce la capacité des individus à jouir de certains droits (liberté d'expression, droit à l'information, etc.), il en fragilise d'autres (droit à l'image, droit à la vie privée, etc.).

Les nouveaux défis lancés par les capacités immenses des technologies de l'information (le stockage des données par exemple) et le caractère transfrontière d'Internet interrogent les droits gravés sur le cylindre de Cyrus ou même, plus récemment, la Déclaration universelle des droits de l'homme de 1948. Il est fort probable que certains droits fondamentaux doivent être réinterprétés à la lumière de la technique contemporaine ou que de nouveaux doivent être établis.

Un groupe de réflexion sur les mutations dans le domaine des technologies et de la communication a donc été créé à l'initiative d'André Santini, ancien Ministre français et Député-maire d'Issy-les-Moulineaux. Le but du groupe, dont le rapporteur était Alain Bensoussan, a été de formuler des recommandations à l'occasion des travaux parlementaires et communautaires en cours. Un livre blanc issu des travaux de ce groupe a été publié, ayant pour ambition de servir de base de travail et d'échanges élargis, afin d'aboutir à terme à une Déclaration des droits de l'homme numérique [3].

1. Tribunal de Grande Instance de Paris, Ordonnance de référé du 22 mai 2000, http ://ww w.legalis.net/spip. php ?page=jurisprudence-decision&id*article=175 ; P. Vackle, C. Uyttendaele, « racisme et négationnisme sur Internet : les affaires Infonie et Yahoo bis » note sous Corr. Bruxelles, 15 janvier 2002, RDTI, 2002, n° 13, p. 73-92.

2. http ://www.lemonde.fr/societe/article/2014/07/15/taubira-comparee-a-un-singe-9-mois-de-prison-ferme-pour-l-ex-candidate-fn*4457839*3224.html.

3. A. Santini, A. Bensoussan, 20 novembre 2000, Droits de l'homme numérique, Livre blanc de la ville d'Issy-Les-Moulineaux.

Cette réflexion a été ensuite approfondie par celle de l'ancienne Secrétaire d'État au développement de l'économie numérique, Nathalie Kosciusko-Morizet, le 12 novembre 2009 [4], ou encore celle du Ministre Hervé Morin le 17 novembre 2009 [5].

Cette prise de conscience des nouveaux enjeux n'a évidemment pas lieu qu'au niveau de la France. Ainsi, depuis la résolution A/HRC/20/L.13 du Conseil des droits de l'homme des Nations Unies du 29 juin 2012 sur la promotion, la protection et l'exercice des droits de l'homme sur l'Internet, l'Organisation des nations unies (ONU) demande aux États d'assurer que les droits dont les personnes jouissent hors ligne soient également protégés en ligne [6].

Le parti-pris de notre contribution est de revisiter les huit droits fondamentaux de l'homme numérique proposés par Hervé Morin en 2009 pour évoquer ce que pourraient être ces nouveaux droits fondamentaux, à savoir :

1. le droit d'utiliser l'Internet ;
2. le droit à la vie privée numérique ;
3. le droit à la dignité numérique ;
4. le droit à la propriété numérique ;
5. le droit à transparence numérique ;
6. le droit à l'anonymat numérique ;
7. le droit à l'oubli ;
8. le droit à une identité numérique.

1 Article 1er : le droit d'utiliser l'Internet

« *Toute personne a le droit d'accéder et d'utiliser librement le réseau Internet, neutre et ouvert, sous réserve de ne pas porter atteinte à l'ordre public et aux droits d'autrui* ».

Ce droit d'accès et d'utilisation est essentiel en ce que l'Internet permet désormais d'accéder à d'innombrables services (information, e-commerce, accomplissement de formalités administratives, fourniture de biens culturels...). L'Internet doit, par conséquent, être considéré comme relevant d'un service public au même titre que le réseau d'énergie, le réseau postal, les réseaux de transports, etc.

L'effectivité du droit d'accès à ce « *service public numérique universel* » implique une couverture géographique satisfaisante et la fourniture d'un service de qualité à un tarif abordable.

Il suffit d'utiliser une fois le réseau de communication électronique congolais, par exemple, pour se rendre compte que nous ne sommes pas tous égaux sur ce point.

Le principe de neutralité de l'Internet implique que toutes les données soient traitées de façon égale sur le réseau de manière à ce que les fournisseurs d'accès à Internet

4. Par son atelier « Droit à l'oubli numérique » organisé dans les locaux de Science Po Paris.
5. http ://www.droits-numeriques.org/la-declaration/la-declaration-des-droits-fondamentaux-numeriques.html.
6. https ://documents-dds-ny.un.org/doc/UNDOC/LTD/G12/147/11/PDF/G1214711.pdf?OpenElement.

acheminent dans les mêmes conditions les données de leurs clients, indépendamment de leur chiffre d'affaire, de leur raison sociale, etc.

Une récente décision de la Federal Communication Commission (FCC), chargée de réguler les télécommunications et l'Internet aux États-Unis, va dans ce sens. En effet, par une décision du 26 février 2015 relative à la neutralité du Net [7], elle a estimé que l'Internet devrait être considéré comme un bien public au même titre que le réseau téléphonique. Partant de ce postulat, la FCC a consacré le principe de neutralité du Net sur tout le territoire nord-américain.

On note également des évolutions relatives à ce sujet sur le Vieux continent. En effet, le règlement européen 2015/2020 établissant des mesures relatives à l'accès à un Internet ouvert a été adopté le 25 novembre 2015 [8]. Ce règlement prévoit l'introduction des premières règles à l'échelle de l'Union européenne visant à préserver l'accès à un Internet ouvert, et donc à assurer la neutralité de l'Internet. Toutefois, la pratique du taux zéro (ou « zero-rating ») qui consiste pour un fournisseur d'accès à ne pas facturer à l'utilisateur final la bande passante utilisée pour accéder à certains services, n'a pas été supprimée par ce texte. Pourtant, certains considèrent que cette pratique risque d'engendrer une discrimination latente dans l'accès à certains services, mettant dès lors en péril l'Internet ouvert.

Pareillement, le Comité des Ministres du Conseil de l'Europe a adopté le 13 janvier 2016 une recommandation (CM/Rec [2016]1) sur la protection et la promotion du droit à la liberté d'expression et du droit à la vie privée en lien avec la neutralité du réseau [9]. Cette recommandation contient des lignes directrices sur la neutralité du réseau, rappelant que le « *trafic Internet devrait traiter de manière égale sans discrimination, restriction, ni ingérence, quels que soient l'émetteur, le destinataire, le contenu, l'application, le service ou le dispositif*[10] ». Ainsi, la recommandation prévoit que cette obligation incombe aux fournisseurs d'accès à l'Internet, qui peuvent y déroger dans certains cas précis [11] (pour l'application d'une décision de justice par exemple).

La recommandation rappelle par ailleurs que le principe de neutralité du réseau est l'une des manifestations des articles 8 (droit au respect à la vie privée et familiale) et 10 (liberté d'expression) de la Convention européenne des droits de l'homme (CEDH)

7. Open Internet Order, Feb 26, 2015, FCC-15-24, https ://www.fcc.gov/document/fcc-releases-open-Internet-order. Le 14 juin 2016, la Cour d'appel a confirmé les règles de « neutralité du net » proposées par la FCC. Les fournisseurs d'accès à Internet, qui s'opposent à cette décision, ont annoncé qu'ils avaient l'intention de saisir la Cour suprême. De même, de nombreux membres du Congrès républicain rejettent ce principe, ainsi que l'autorité de la FCC dans ce domaine.

8. Règlement (UE) 2015/2020 du Parlement européen et du Conseil du 25 novembre 2015 établissant des mesures relatives à l'accès à un Internet ouvert et modifiant la directive 2002/22/CE concernant le service universel et les droits des utilisateurs au regard des réseaux et services de communications électroniques et le règlement (UE) no 531/2012 concernant l'itinérance sur les réseaux publics de communications mobiles à l'intérieur de l'Union, JOUE, 26 novembre 2015, L 310, p. 1-18. L'Office de l'organe des régulateurs européens des communications électronique a présenté le 6 juin 2016 son projet de lignes directrices sur la neutralité de l'Internet ; un projet soumis à consultation publique jusqu'au 18 juillet 2016, pour une publication fin août 2016. Ces lignes directrices ont pour objectif de préciser les modalités concrètes d'application du règlement.

9. https ://search.coe.int/cm/Pages/result*details.aspx ?ObjectID=09000016805c1ecd.

10. Point 2.1 de la recommandation précitée.

11. Point 2.2, *ibid.*

en ce que, s'il est porté atteinte au principe de neutralité, cela conduirait par ricochet à la violation des articles précités de la CEDH.

Le droit à une libre utilisation du réseau s'oppose à toute forme de filtrage par les pouvoirs publics, sauf pour des motifs d'ordre public comme, par exemple, la lutte contre la pédophilie.

Le filtrage généralisé opéré par la Chine ou la Turquie, par exemple, n'entre pas dans cette exception et n'est évidemment pas acceptable.

Le Conseil des droits de l'homme des Nations Unies a adopté, le 1er juillet 2016, une résolution A/HRC/32/L. 20 [12] qui condamne sans équivoque les mesures visant à empêcher ou à perturber délibérément l'accès à l'information ou la diffusion d'informations en ligne et invite tous les États à s'abstenir de telles pratiques et à les faire cesser.

Dans ce texte, le Conseil rappelle également les articles 9 et 21 de la Convention relative aux droits des personnes handicapées, qui invitent notamment les États parties à prendre des mesures appropriées pour promouvoir l'accès des personnes handicapées aux nouveaux systèmes et technologies de l'information et de la communication, y compris à l'Internet.

L'utilisation du réseau peut également être encadrée en cas d'atteinte aux droits d'autrui. Ceci peut justifier un accès restreint au réseau dans le cadre professionnel afin de limiter la navigation sur Internet aux seules exigences liées à l'activité professionnelle. On vise ici le contrôle encadré de l'usage des communications électroniques sur le lieu du travail.

2 La vie privée numérique

« *Toute personne a droit au respect de sa vie privée numérique et au secret de ses échanges numériques. Les systèmes d'information personnels sont assimilés au domicile privé* ».

Les systèmes d'information faisant l'objet d'un accès personnalisé et sécurisé (messagerie électronique, outils mobiles, réseaux sociaux, etc.) doivent être assimilés à un domicile privé numérique dont la violation doit être sanctionnée.

Dans son arrêt *Niemietz* rendu le 16 février 1992, la Cour européenne des droits de l'homme a consacré l'existence d'un droit au respect de la vie privée du travailleur sur le lieu du travail. La révolution numérique n'a pas conduit à un revirement de cette jurisprudence [13]. L'usage de l'informatique ne doit pas porter atteinte à la vie privée y compris sur le lieu de travail.

12. https ://documents-dds-ny.un.org/doc/UNDOC/LTD/G16/131/90/pdf/G1613190.pdf ?OpenElement/

13. Arrêt Niemietz c. Allemagne, 16 décembre 1992 ; Arrêt Halford c. Royaume-Uni, 25 juin 1997 ; Arrêt Kopp c. Suisse, 24 mars 1998 ; Arrêt Amann c. Suisse, 16 février 2000 ; Arrêt Copland c. Royaume-Uni, 3 avril 2007.

La protection de l'intimité numérique implique également le respect d'obligations particulières de sécurité s'agissant d'informations confidentielles, relevant par exemple du secret médical ou fiscal auxquelles seuls des tiers autorisés doivent avoir accès.

Le respect de la vie privée numérique peut justifier la mise en place de systèmes de chiffrement et d'accès protégé par mot de passe. Se pose dès lors la question des *backdoors*. Il s'agit de points d'accès confidentiels, à un programme ou à un service en ligne. Ces « portes dérobées » secrètes peuvent parfois être utilisées à mauvais escient par certaines personnes, tels les pirates informatiques, les chefs d'États totalitaires ou les patrons qui tentent de contrôler les salariés.

La surveillance de masse a été encadrée par l'arrêt *Digital Rights Ireland Ltd & Michael Seitlinger e.a.* rendu par la Cour de justice de l'Union européenne en date du 8 avril 2014 [14]. Il s'agissait de deux renvois préjudiciels visant à savoir si les données de communication des abonnés et utilisateurs pouvaient être conservées. La Cour a estimé que l'obligation de conservation imposée par la Directive 2006/24/CE portait atteinte au régime de protection du droit au respect de la vie privée découlant des directives 95/46 et 2002/58 sur les traitements de données à caractère personnel.

Malheureusement, les velléités des gouvernements n'ont absolument pas été bridées par cet arrêt.

Un recours constitutionnel contre la loi belge de transposition de cette même directive a abouti à un arrêt d'annulation du 11 juin 2015 [15]. Un mois et demi après cet arrêt, un projet de loi était rédigé afin de continuer à surveiller tous les Belges sans distinction pour des infractions de 6 mois et plus, dans le mépris du secret professionnel [16]. Le législateur belge soutient que la Cour de justice et la Cour constitutionnelle n'auraient rien compris et que, certes l'article 8 de la CEDH s'oppose à cette loi mais qu'il n'y aurait pas moyen de s'y conformer. Un nouveau recours est donc envisageable.

La France, en suite des différents attentats dont elle a été victime, n'est pas restée en marge de ce mouvement. La Loi n° 2015-912 du 24 juillet 2015 relative au renseignement [17] (ci-après Loi renseignement) a été présentée par le Premier Ministre Manuel Valls comme étant une nécessité pour contrecarrer les attaques terroristes. Elle a été sujette à des critiques virulentes qui l'ont portée devant le Conseil constitutionnel. Ce dernier n'a censuré que quelques dispositions, en validant d'autres beaucoup plus critiquables. On dénombre notamment le nouvel article L.851-3 du Code de la sécurité intérieure qui met en place le système des « boîtes noires », consistant en l'installation sur les réseaux et les serveurs d'instruments destinés à scanner les trafics téléphoniques et Internet de tous les utilisateurs indistinctement, dans le but de détecter des communications suspectes en lien avec une menace terroriste. Tous les utilisateurs voient ainsi leurs données collectées, sans même savoir qu'ils sont espionnés.

14. http ://curia.europa.eu/juris/document/document.jsf ?docid=150642&doclang=FR.
15. http ://www.const-court.be/public/f/2015/2015-084f.pdf.
16. Ce projet a aujourd'hui été adopté sous la forme de la loi du 29 mai 2016 relative à la collecte et à la conservation des données dans le secteur des communications électroniques, M.B., 18 juillet 2016.
17. https ://www.legifrance.gouv.fr/affichTexte.do ?cidTexte=JORFTEXT000030931899&categorieLien =id.

Plus critiquable encore est l'article L. 811-3 du même Code (inséré par l'article 2 de la Loi renseignement) qui énonce que le Premier Ministre peut autoriser les services de renseignements à recourir à des mesures de surveillance intrusives pour des raisons édictées en des termes très généraux et indéfinis. Ainsi, il sera possible de recourir aux techniques de renseignements en raison d'« *intérêts majeurs de la politique étrangère* », « *la prévention des atteintes à la forme républicaine des institutions* », ou encore de « *la prévention des violences collectives de nature à porter gravement atteinte à la paix publique* ». Il est indéniable que ces raisons risquent de servir de base légale pour justifier la surveillance de masse au nom de n'importe quel motif. C'est d'ailleurs pour cela qu'un nombre conséquent d'organisations s'est opposé à ce texte [18] (Amnesty International France, la Ligue des droits de l'homme, le Syndicat de la Magistrature, le Syndicat des Avocats de France, etc. [19]).

La résolution 69/166, adoptée par l'Assemblée générale de l'ONU le 18 décembre 2014, sur le droit à la vie privée à l'ère du numérique [20] appelle pourtant les États à revoir leurs procédures, leurs pratiques et leur législation en matière de surveillance et d'interception des communications et de collecte de données personnelles, notamment à grande échelle, dans le souci de défendre le droit à la vie privée en veillant à respecter pleinement et effectivement toutes leurs obligations au regard du droit international.

3 Article 3 : la dignité numérique

« *La dignité numérique est un droit fondamental* ».

Jean Pradel définit dans son ouvrage *Droit pénal spécial* les infractions portant atteinte à la dignité comme « *celles qui, hors les cas d'attentat à la vie, à l'intégrité ou à la liberté, ont pour effet essentiel de traiter la personne comme une chose, comme un animal ou, dans le meilleur des cas, comme un être auquel serait dénié tout droit à l'honneur et à son honorabilité* [21] *»*.

En France, le principe de dignité a été élevé au rang de principe à valeur constitutionnelle par la décision du Conseil constitutionnel relative à la Loi bioéthique [22]. Ce principe est également consacré par la Charte des droits fondamentaux de l'Union européenne en son article 1[er] [23].

C'est donc manifestement un principe important qu'il convient de respecter aussi bien dans la vie « moléculaire » que dans la vie numérique.

On parle, dans le cadre du cyberespace, du principe de dignité numérique. Il s'agit du refus de porter atteinte à la dignité humaine à travers l'Internet. La consécration de ce principe est d'autant plus importante que la circulation des images et des informations dans cet espace est immédiate et éparse.

18. http ://www.amnesty.fr/Nos-campagnes/Liberte-expression/Actualites/La-loi-sur-le-renseignement-doit-etre-declaree-inconstitutionnelle-15641
19. https ://sous-surveillance.fr/#/
20. http ://www.un.org/fr/documents/view*doc.asp ?symbol=A/RES/69/166
21. Pradel Jean, *Droit Pénal Spécial*, Paris, Cujas, 2014, 788 p.
22. Décision n° 94-343/344 DC du 27 Juillet 1994, voir le considérant n° 2.
23. Art 1[er] Charte des droits fondamentaux de l'Union Européenne : « *La dignité humaine est inviolable. Elle doit être respectée et protégée* ».

L'Internet peut être l'instrument d'atteinte à la dignité humaine mais il est en réalité souvent plutôt le démultiplicateur d'atteinte à la dignité.

D'après l'étude *Ipsos Junior Connect 2015* [24], le temps moyen par semaine sur Internet des enfants âgés de 1 à 6 ans était de 3h 40 min en 2015 contre 2h 10 minutes en 2012. Ces nouvelles habitudes justifient donc une extrême vigilance afin de prévenir toute atteinte à la dignité numérique des plus jeunes.

Le respect de la dignité humaine dans la sphère numérique suppose le refus d'utilisation de qualificatifs contraires à l'ordre public et aux bonnes mœurs. La dignité humaine est aussi liée à la notion de respect.

Certes, il n'existe pas pour l'Internet, à la différence du secteur audiovisuel, d'autorité de régulation des contenus mis en ligne. Mais cela ne doit pas conduire à autoriser sur la toile ce qui est interdit sur les autres supports de communication. Les publications sur Internet des photos de la pendaison de Saddam Hussein, ou encore les photos intimes volées de Laure Manaudou restent inacceptables.

4 La propriété numérique

« *Toute personne est propriétaire des informations numériques la concernant, dans le respect des droits et libertés d'autrui. L'usage de ces informations est défini par la personne concernée* ».

Afin de combler le déficit des législations relatives à la protection des données à caractère personnel (méconnues, complexes, etc.), on pourrait imaginer, à l'instar de ce qui est proposé par Alain Bensoussan [25], de considérer les données émanant d'une personne – non seulement le nom ou les coordonnées, mais également les habitudes de consommation, etc. – comme des « produits » (au sens du droit des biens, toutefois sans altération de la substance de la personne) de sa personnalité, produits devenant des choses susceptibles de propriété au sens du Code civil.

Certains éminents auteurs parlent d'ailleurs, de longue date, des « *biens de la personnalité* » en abordant les questions de protection des données à caractère personnel, comme la protection du nom patronymique [26]. Dans cette hypothèse, contenant et contenu se confondraient et seraient considérés comme un tout, à l'instar de certaines œuvres graphiques couvertes par le droit d'auteur.

Il est nécessaire de clarifier le statut juridique des données personnelles disponibles dans la sphère numérique. En effet, chaque individu devrait pouvoir maîtriser son identité informationnelle, tant biologique que numérique.

Le développement conséquent des sites de partages des données nous mène à nous questionner sur la propriété et les conditions d'utilisation des données disponibles. La propriété numérique reconnaît ainsi à toute personne physique et morale un droit de propriété sur les informations numériques la concernant. Il en découle, d'une part, un

24. http ://fr.slideshare.net/IpsosFrance/junior-connect-la-conqute-de-lengagement, slide n° 13.

25. Santini André, Bensoussan Alain, 20 novembre 2000, http ://www.alain-bensoussan.com/wp-content/uploads/39889121.pdf, Droits de l'homme numérique, Livre blanc de la Ville d'Issy les Moulineaux.

26. Rigaux François, 2004, T. 9, p. 827, Protection de la vie privée, RPDB.

droit d'accès permanent et de rectification de ces données et, d'autre part, un droit de retrait de ces données.

Les personnes concernées (dont les données ont été collectées, et de manière plus globale traitées) doivent être préalablement informées de leurs droits, conformément au principe de transparence numérique, par le biais de « conditions générales d'utilisation » accessibles et respectueuses de la dignité numérique et du droit à l'oubli.

La reconnaissance de ce droit de propriété n'entraîne pas automatiquement un droit à rémunération puisque les données personnelles sont généralement mises à disposition avec le consentement (plus ou moins éclairé – mais généralement inconscient) de la personne physique ou morale concernée.

La Cour de justice de l'Union européenne a statué dans le sens d'un droit de propriété sur les données numériques dans un arrêt du 3 juillet 2012, rendu sur deux questions préjudicielles posées à l'occasion d'un litige entre un éditeur de logiciel et un revendeur de logiciels d'occasion [27]. L'enjeu portait sur l'interprétation de la Directive 2009/24 du 23 avril 2009, concernant la protection juridique des programmes d'ordinateur dans l'hypothèse de revente de licence d'occasion sur des logiciels à télécharger et, singulièrement, sur la notion d'épuisement du droit de distribution après la première vente.

La Cour s'est tout d'abord attachée à définir le concept de « vente » au sens de l'article 4, paragraphe 2, de la Directive 2009/24 et le définit comme étant la « *convention par laquelle une personne cède, moyennant le paiement d'un prix, à une autre personne ses droits de propriété sur un bien corporel ou incorporel lui appartenant* ». Il s'en déduit un droit de propriété sur le programme d'ordinateur et les données qui composent celui-ci.

Confrontée à l'argumentation de l'éditeur, décomposant la vente en mise à disposition gratuite du logiciel et conclusion d'un contrat de licence onéreux, la Cour a estimé qu'il fallait envisager l'opération dans son ensemble comme un transfert du droit de propriété sur la copie du programme d'ordinateur, et ce que le logiciel soit téléchargé ou présent sur un support matériel comme un CD-ROM ou un DVD.

La première vente d'un logiciel, même sans support matériel, entraine donc l'épuisement du droit de distribution de cette copie et l'éditeur de logiciel perd la possibilité d'invoquer son monopole d'exploitation pour s'opposer à la revente de cette copie.

La Cour précise également que la revente de la copie implique nécessairement que le vendeur rende inutilisable son exemplaire du logiciel, à défaut de quoi il violerait le droit exclusif de reproduction de l'éditeur.

Si l'on étendait ce raisonnement à la propriété des données personnelles, on pourrait considérer que dès lors que le propriétaire des données personnelles, c'est-à-dire la personne concernée, décide de vendre ses données personnelles, elles ne lui appartiendraient plus.

27. CJUE, UsedSoft GmbH c. Oracle International Corp. , 3 juillet 2012, C-128/11.

Cette approche risquerait de mettre en péril le contrôle des personnes concernées sur leurs données personnelles.

De surcroît, des critiques se sont élevées à l'encontre de cette proposition [28] : le fait d'attribuer un droit de propriété sur les données à caractère personnel reviendrait à nier le caractère de droit fondamental de la protection de la vie privée, puisqu'un droit de propriété implique une dépossession incompatible avec le caractère inaliénable des droits de la personnalité.

Cela renforcerait le clivage social dès lors que les plus pauvres seraient plus enclins à céder leurs données pour bénéficier de services gratuits ou de réductions alors que les plus riches pourraient plus facilement accéder à des services payants peut-être plus respectueux de leur vie privée.

Se poserait également la question de la titularité sur les données « dérivées » ou « enrichies », comme l'examen des habitudes de consommation, par opposition aux données « brutes » comme les coordonnées. Ces données enrichies étant issues de l'analyse et du travail de l'entreprise et donc le fruit de son investissement propre, le sujet de l'analyse pourrait-il revendiquer un droit de propriété sur ces données, qui contiennent la vraie valeur économique ?

La question de la valeur économique est également mise en avant comme critique de la propriété sur les données. *Per se*, des données n'auraient aucune valeur, cette dernière ne pouvant s'évaluer que par rapport à un traitement ou un usage spécifique.

Enfin, une telle approche aurait les mêmes limites juridiques et pratiques que celles généralement attribuées au droit d'auteur.

Il est certain que la mise en place pratique d'un droit de propriété sur les données entrainerait son lot de difficultés pratiques, dont la plupart sont déjà effectivement rencontrées en matière de droit d'auteur. Nul ne peut toutefois nier que le système actuel de protection des données à caractère personnel présente un degré de complexité particulièrement élevé et est, par rapport à son ancienneté, particulièrement peu implémenté dans les pratiques quotidiennes des entreprises et des particuliers. Le recours aux mécanismes de la propriété qui sont, à tout le moins intuitivement, bien connus du grand public permettrait probablement une meilleure intégration de la protection des données.

L'argument de la valeur économique est plus étrange dès lors qu'aucune chose n'a de valeur en soi. Un bien ne peut être évalué que par rapport à un usage qui peut en être fait ou parce qu'un consensus social, exprimé à travers un marché, lui assigne une valeur d'échange. Comme toute chose, la donnée numérique devra faire l'objet d'une évaluation et la pratique quotidienne de la vente et de l'échange de bases de données démontre bien qu'un marché existe et que le prix d'une donnée peut être chiffré à travers celui-ci.

En ce qui concerne le clivage social qui serait généré ou aggravé par cette extension du droit de la propriété, force est de constater que celui-ci existe déjà et ce, malgré

28. CNIL, n° 1, p. 55-56, Vie privée à l'horizon 2020. Paroles d'experts, Cahiers IP, http ://www.cnil.fr/fileadmin/documents/LaCNIL/publications/DEIP/CNIL-CAHIERSIPn1.pdf.

les initiatives pédagogiques prises par les autorités nationales de protection de la vie privée. À l'heure actuelle, les populations les plus pauvres – outre qu'elles ignorent le plus souvent leurs droits – cèdent, généralement à leur insu, la maîtrise sur leurs données à caractère personnel afin de bénéficier de services gratuits ou d'offres promotionnelles. D'un point de vue pédagogique, utiliser le mécanisme de la propriété sur les données à caractère personnel permettrait de donner conscience à tous de la valeur financière de ces données. Cette prise de conscience susciterait probablement une modification d'attitude de la population, soit que celle-ci refuserait les traitements, soit qu'elle réclamerait une meilleure contrepartie.

L'argument lié à la propriété des données « enrichies » est plus ardu à rencontrer, singulièrement dans l'hypothèse de déploiement de technologies de type Big Data. Les données « enrichies » ou « dérivées » résultent de l'analyse et du traitement de données « brutes ». Elles ne peuvent donc, en théorie, être créées sans l'autorisation du titulaire de ces données « brutes ». Si celui-ci autorise la création de ces données « enrichies », elles lui appartiennent en vertu du droit d'accession contenu à l'article 546 du Code civil, les données « enrichies » étant des produits de sa personne (sans perte de substance).

Cependant, la propriété ne sera acquise au titulaire de ces données enrichies que pour autant qu'il indemnise les travaux des tiers, en vertu de l'article 548 du Code civil belge. Il s'agit toutefois d'un faux problème, puisque c'est le tiers qui a intérêt à produire ces données enrichies et qu'il ne devrait par conséquent pas réclamer d'indemnisation au titulaire.

Il ne faut toutefois pas perdre de vue les règles contenues dans les articles 570, 571 et 572 du Code civil belge [29] qui prévoient les hypothèses d'utilisation d'une matière appartenant à autrui pour former une chose d'une nouvelle espèce. Dans ce cas, si la valeur de la main-d'œuvre surpasse de beaucoup la valeur de la matière, l'ouvrier aurait le droit de retenir la chose travaillée en remboursant le prix de la matière au propriétaire.

En l'occurrence, et singulièrement dans les hypothèses de Big Data mettant en jeu des algorithmes complexes et de grandes quantités de coûteuse puissance de calcul, ces règles pourraient éventuellement être invoquées par les entreprises effectuant des traitements de données pour justifier des traitements « sauvages » et s'approprier des informations « enrichies », en indemnisant *a minima* les propriétaires originaires.

29. Art. 570 : « *Si un artisan ou une personne quelconque a employé une matière qui ne lui appartenait pas, à former une chose d'une nouvelle espèce, soit que la matière puisse ou non reprendre sa première forme, celui qui en était le propriétaire a le droit de réclamer la chose qui en a été formée, en remboursant le prix de la main-d'œuvre* ».

Art. 571 : « *Si cependant la main-d'œuvre était tellement importante qu'elle surpassât de beaucoup la valeur de la matière employée, l'industrie serait alors réputée la partie principale, et l'ouvrier aurait le droit de retenir la chose travaillée, en remboursant le prix de la matière au propriétaire* ».

Art. 572 : « *Lorsqu'une personne a employé en partie la matière qui lui appartenait, et en partie celle qui ne lui appartenait pas, à former une chose d'une espèce nouvelle, sans que ni l'une ni l'autre des deux matières soit entièrement détruite, mais de manière qu'elles ne puissent pas se séparer sans inconvénient, la chose est commune aux deux propriétaires, en raison, quant à l'un, de la matière qui lui appartenait ; quant à l'autre, en raison à la fois et de la matière qui lui appartenait, et du prix de sa main-d'œuvre* ».

Le marché des données permettra peut-être de pallier cet inconvénient en fixant une valeur élevée aux données « brutes » à partir desquelles les données « enrichies » sont déduites.

5 La transparence numérique

« Toute personne a le droit d'être informée de l'existence des informations numériques la concernant ».

La transparence numérique suppose que l'individu puisse connaître le contenu des éléments constitutifs de sa personnalité biologique et numérique.

Cela conduit à l'exercice d'une citoyenneté numérique de laquelle résulte la possibilité pour l'individu :

- de maîtriser les informations à caractère personnel qui le concernent ;
- d'être informé sur ses droits ;
- d'exprimer un consentement préalable, sauf dérogation, à la gestion de ses données personnelles ;
- de limiter l'usage des données personnelles à des finalités légitimes et proportionnées ;
- de connaître l'ensemble des informations le concernant détenues par toutes personnes opérant sur des données.

Le secret professionnel ayant vocation à protéger la personne, il ne saurait être utilisé à son encontre pour s'opposer à l'application du principe de transparence par le client.

L'actuelle « Loi renseignement » française va totalement à l'encontre de ce principe de transparence, puisqu'elle permet le traitement de données personnelles à l'insu des personnes concernées, les empêchant ainsi d'effectuer un quelconque contrôle sur leurs données. Cependant, si cette loi va à l'encontre de ce principe, le projet de loi pour une République numérique [30] paraît quant à lui apporter certaines garanties allant dans le sens de la transparence numérique. Parmi les principes que ce projet de loi consacre, on dénombre la portabilité des données [31], le principe de loyauté des plateformes de services numériques et le droit de récupération des données personnelles.

6 Article 6 : l'anonymat numérique

« Le droit à l'anonymat numérique gratuit est reconnu à toute personne, sous réserve de ne pas porter atteinte à l'ordre public et aux droits et libertés d'autrui ».

Dans une démocratie, l'anonymat conditionne l'exercice de libertés comme celle d'aller et de venir, d'expression ou de culte, etc.

30. http ://www.gouvernement.fr/action/pour-une-republique-numerique.

31. L'article 20 du Nouveau Règlement général relatif à la protection des données à caractère personnel (Règlement UE 2016/679 du 27 avril 2016) a récemment consacré le droit à la portabilité des données.

Le droit à l'anonymat sur Internet fait partie de la liberté d'expression constitutionnellement garantie par la Loi Fondamentale allemande. C'est ce qu'énonce clairement la Cour d'appel de Hamm par un arrêt rendu le 3 août 2011 [32].

L'anonymat ici visé est en réalité une possibilité de pseudonymat, qui n'exonère aucunement celui qui y a recours de sa responsabilité à l'égard des propos illégaux (diffamation, injure, appel à la haine, etc.).

Sur l'Internet, l'utilisation de pseudonymes permet de dissimuler son identité réelle sans pour autant être assuré qu'aucun lien ne sera établi entre son identité numérique et son identité biologique.

Seules des raisons d'ordre public ou d'atteintes aux droits d'autrui sont de nature à justifier la levée de l'anonymat, sous le contrôle d'une autorité judiciaire.

L'affaire Eolas [33] démontre que le système français du pseudonymat de l'article 6-III-2, alinéa 1, de la loi pour la confiance dans l'économie numérique [34] peut fonctionner correctement : le Conseil de l'ordre des avocats ne peut y porter atteinte mais un tribunal correctionnel a cette possibilité.

Plus en amont, mais toujours sous le contrôle d'une autorité judiciaire, la Cour de justice a jugé dans une affaire mettant en jeu des violations de droits d'auteur commises par un utilisateur *via* le réseau Wi-Fi ouvert et gratuit d'un magasin, qu'une injonction ordonnant la sécurisation de la connexion à Internet au moyen d'un mot de passe est de nature à assurer un équilibre entre, d'une part, les droits de propriété intellectuelle des titulaires de droits et, d'autre part, le droit à la liberté d'entreprise des fournisseurs d'accès et le droit à la liberté d'information des utilisateurs du réseau. La Cour relève, en particulier, qu'une telle mesure est susceptible de dissuader les utilisateurs d'un réseau de violer des droits de propriété intellectuelle. À cet égard, la Cour souligne néanmoins que, afin d'assurer la réalisation de cet effet dissuasif, il est nécessaire que les utilisateurs, pour éviter qu'ils n'agissent anonymement, soient obligés de révéler leur identité avant de pouvoir obtenir le mot de passe requis [35].

La reconnaissance d'un droit à l'anonymat numérique suppose qu'il soit proposé gratuitement à ses bénéficiaires. Or, les exemples restent nombreux où l'anonymisation revêt un caractère payant, à l'instar du surcoût de 5 euros appliqué au « Passe Navigo Découverte » anonyme, vendu aux usagers des transports en commun franciliens.

Certains évènements nous poussent à nous questionner sur la réalité actuelle de l'anonymat de manière plus globale. Le cas de la fausse alerte à la bombe en 2013 à l'Université de Harvard est emblématique, dès lors qu'on a retrouvé les traces de la personne ayant lancé l'alerte de manière anonyme. Il s'agissait d'un étudiant de l'uni-

32. Oberlandesgericht Hamm, 3 août 2011, I-3 U 196/10, http ://www.justiz.nrw.de/nrwe/olgs/hamm/j2011/I*3*U*196*10beschluss20110803.html.

33. Corr. Paris, ch. presse, 6 octobre 2015, Me Eolas/IPJ, sans se prononcer sur le fond de l'affaire toutefois.

34. Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique.

35. CJUE, 15 septembre 2016, C-484/14, Tobias Mc Fadden / Sony Music Entertainment Germany GmbH, http ://curia.europa.eu/juris/document/document.jsf ;jsessionid=9ea7d2dc30d5d6d1f3f9cfc945d2b91dbba49fe0b00e.e34KaxiLc3qMb40Rch0SaxyKa3z0 ?text=&docid=183363&pageIndex=0&doclang=FR&mode=req&dir=&occ=first&part=1&cid=222883.

versité ayant envoyé un courriel aux services de sécurité de l'établissement *via* une messagerie anonyme en passant par le réseau TOR (*The Onion Router*) qui permet de camoufler les traces sur Internet. Malgré le recours à cet outil, l'étudiant a pu être retrouvé, ce qui amène le Professeur Jean-Paul Pinte à ce constat : « *il est impossible d'être anonyme sur Internet*[36] ».

Il y a donc aujourd'hui une véritable difficulté : on devrait avoir droit à un véritable anonymat sans passer par l'utilisation d'outils compliqués ou le paiement d'un prix. L'anonymat devrait être la norme sur la toile, comme dans la vie réelle. Ce droit devrait donc être consacré au plus vite afin de permettre aux lanceurs d'alertes, aux citoyens lambda, plus particulièrement à ceux vivant sous des régimes dictatoriaux, d'être libres à tout le moins dans le cyberespace.

7 Article 7 : le droit à l'oubli

« *Toute personne a le droit de retrait des informations dont elle est propriétaire ou la concernant, sous réserve de ne pas porter un préjudice grave aux personnes physiques ou morales détenant lesdites informations et de ne pas nuire au devoir d'information générale et de réalité historique* ».

On pourrait dire que les données stockées sur la toile ont une durée de vie « infinie ». En effet, l'Internet soulève un problème d'imprescriptibilité des données. La vie professionnelle et privée n'est pourtant supportable que parce que les tiers et nous-mêmes oublions nos erreurs.

Ce droit fondamental est en passe d'être reconnu. C'est tout d'abord un droit au déréférencement, qui a été consacré par la Cour de justice de l'Union européenne dans l'arrêt Google Spain, en date du 13 mai 2014[37].

En 2010, un citoyen espagnol constate que les recherches associées à son nom *via* le moteur de recherche Google, renvoyaient vers deux pages du quotidien *La Vanguardia*, datés de 1998, mentionnant son nom pour une vente aux enchères immobilière liée à une saisie pratiquée en recouvrement de dettes de sécurité sociale. L'affaire étant close depuis de nombreuses années, et considérant que ces informations étaient obsolètes – et dégradaient certainement son image – l'intéressé décida d'introduire une réclamation auprès de l'Autorité espagnole de protection des données à l'encontre de *La Vanguardia* et de Google, dans le but d'obtenir la suppression des pages Web et leur désindexation dans les résultats de recherche de Google. L'Agence de protection des données rejeta la réclamation dirigée contre *La Vanguardia* mais demanda à Google de prendre les mesures nécessaires pour retirer les données de son index. C'est alors que Google Spain et Google Inc. saisirent la juridiction d'appel (*Audiencia nacional*) afin d'obtenir l'annulation de la décision de l'Autorité espagnole de protection des données.

36. http ://o.nouvelobs.com/high-tech/20140124.OBS3696/pourquoi-vous-ne-serez-jamais-anonyme-sur-Internet.html, entretien de Boris Manenti avec Jeau-Paul Pinte et Stéphane Bortzmeyer.

37. CJUE, 13 mai 2014, Google Spain, C-131/12, http ://curia.europa.eu ; disponible également gratuitement en ligne sur le site http ://jlmbi.larcier.be.

C'est dans un tel contexte que la Cour de justice, saisie dans le cadre d'une question préjudicielle émanant de l'*Audiencia nacional,* rendit un arrêt novateur en termes de protection des données personnelles. Il s'agissait de répondre à plusieurs questions, mais l'enjeu principal était de savoir notamment :

- si les internautes avaient un droit à l'effacement fondé sur le droit européen de la protection des données à caractère personnel ;
- si les législations espagnole et européenne s'appliquaient à Google.

La Cour espagnole constate, d'une part, que le moteur de recherche Google relève de la société Google Inc., société mère du groupe, dont le siège social est aux États-Unis et, d'autre part, que le groupe Google dispose d'une filiale espagnole chargée de la vente en Espagne d'espaces publicitaires, dont les activités sont distinctes de celles d'un moteur de recherche.

Interpelée donc par le fait que l'activité exercée en Espagne n'était pas celle de la personne morale qui traite les données personnelles, l'*Audiencia Nacional* a interrogé la Cour de justice de l'Union européenne à propos du champ d'application territorial des normes européennes relatives à la protection des données personnelles (Directive 95/46/CE sur la protection des données personnelles).

La Cour de justice a estimé que la directive était applicable dès lors qu'une société-mère, effectuant un traitement de données personnelles en dehors de l'Union européenne, avait une filiale établie dans l'Union européenne dont l'activité était la vente et la promotion d'espaces publicitaires qui finançait l'activité de moteur de recherche (qui serait impossible sans ce financement). Par conséquent, il a été établi que les normes européennes issues de la Directive 95/46/CE étaient opposables à Google Inc. !

En sus, la Cour de justice a consacré un droit à l'effacement [38] en considérant que « *l'exploitant d'un moteur de recherche est obligé de supprimer de la liste de résultats, affichée à la suite d'une recherche effectuée à partir du nom d'une personne, des liens vers des pages Web, publiées par des tiers et contenant des informations relatives à cette personne,* [...] *même lorsque leur publication en elle-même* [...] *est licite* ». Elle poursuit, en ajoutant que ces droits prévalent sur « *l'intérêt économique de l'exploitant du moteur de recherche* » ainsi que « *sur l'intérêt* [du] *public à accéder à ladite information* », sauf si, en raison du « *rôle joué par ladite personne dans la vie publique* », « *l'ingérence dans ses droits fondamentaux est justifiée par l'intérêt prépondérant dudit public* ».

38. Pour certains auteurs, il est plus question d'un droit à l'effacement qu'un droit à l'oubli, puisque les données ne sont pas totalement supprimées. En effet, ici la Cour consacre la désindexation d'un lien dans les résultats du moteur de recherche, le contenu présent sur le site Web en cause restant accessible. A. Cassart, J.-F. Henrotte "Arrêt Google Spain : la révélation d'un droit à l'effacement plutôt que la création d'un droit à l'oubli", *JLMB*, 2014/25, p. 1183 et s. disponible gratuitement en ligne sur le site http ://jlmbi.larcier.be. Cela dit, le nouveau Règlement (UE) 2016/679 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (dit Règlement général sur la protection des données), consacre dans son article 17 le droit à l'oubli, qu'il nomme également « droit à l'effacement ».

L'Union européenne a fait un pas de plus en adoptant le Règlement général sur la protection des données personnelles [39].

En effet, l'article 17 du Règlement général sur la protection des données consacre un droit à l'effacement, également qualifié de « droit à l'oubli ».

Ce droit peut être mis en œuvre non seulement lorsque les données ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées, mais également en cas de retrait du consentement au traitement ou d'opposition de la personne concernée. Une plus ample protection est même conférée lorsque le consentement a été donné à l'époque où la personne concernée était mineure.

Cependant, ce droit n'est pas sans limite. Effectivement, comme le prévoit l'article 17 du nouveau Règlement général sur la protection des données, la conservation des données peut se justifier, entre autres, pour des traitements à des fins historiques, statistiques ou scientifiques.

Enfin, et cela accroit évidemment l'effectivité concrète du droit, le responsable du traitement est tenu d'informer les autres responsables du traitement qui traitent ces données suite à leur communication, qu'il convient d'effacer tout lien vers ces données, ou toute copie ou reproduction de celles-ci.

Un dernier pas a été accompli par la Cour de cassation de Belgique qui, par un arrêt du 29 avril 2016 [40], a décidé que « *l'archivage numérique d'un article ancien de la presse écrite ayant, à l'époque des faits, légalement relaté des évènements du passé désormais couverts par le droit à l'oubli ainsi entendu n'est pas soustrait aux ingérences que ce droit peut justifier dans le droit à la liberté d'expression. Ces ingérences peuvent consister en une altération du texte archivé de nature à prévenir ou réparer une atteinte au droit à l'oubli* ». La Cour poursuit, en estimant que le maintien en ligne de l'article en question de manière non anonyme, de nombreuses années après les faits, est de nature à causer un préjudice disproportionné par rapport aux avantages liés au respect strict de la liberté d'expression. C'est pourquoi les juges de la Cour de justice ont estimé que « *les conditions de légalité, de légitimité et de proportionnalité imposées par l'article 10, 2, de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales à toute limitation de la liberté d'expression sont en l'espèce réunies* ».

Contrairement à la Cour de cassation française qui n'a pas fait droit à une demande similaire par un arrêt rendu le 12 mai 2016 [41], la Cour de cassation belge estime que le droit à l'oubli est une composante de l'article 8 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales. L'approche belge appréhende donc le droit à l'oubli comme un droit fondamental (et non comme une

39. Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), JOUE, 4 mai 2016, L 119, p. 1-88.

40. Cass. b., 29 avril 2016, C.15.0052.F, http ://jure.juridat.just.fgov.be/pdfapp/download*blob ?idpdf=F-20160429-1.

41. Cass. fr, 1re ch. Civ., 12 mai 2016, 15-17.729, inédit, https ://www.legifrance.gouv.fr/affichJuriJudi.do ?idTexte=JURITEXT000032532166.

simple composante du droit à la protection des données à caractère personnel, comme l'a fait la juridiction suprême française).

8 Article 8 : l'identité numérique

« *Toute personne a droit à une identité numérique* ».

L'identité numérique est définie par le Professeur Milad Doueihi, Titulaire de la Chaire d'humanisme numérique à l'Université Paris-Sorbonne, comme la « *représentation numérique d'un utilisateur individuel dans un environnement réseau*[42] ».

L'identité numérique d'un utilisateur se construit au fur et à mesure des données personnelles associées à son ou ses profils, des informations qu'il publie sur l'Internet, et des informations que d'autres publient à son sujet.

L'identité numérique n'est pas propre à la personne physique, une personne morale peut pareillement en posséder une, *via* un nom de domaine. Il s'agit d'un nom unique que l'internaute choisit pour lui-même ou son organisation afin de lui conférer une identité, une existence sur l'Internet. Il permet ainsi aux autres internautes de trouver aisément l'organisation ou la personne concernée sur la toile.

Cette identité est parfois la condition *sine qua non* pour l'accès au service public. C'est le cas depuis peu dans l'Hexagone avec *France Connect* qui est « *un système d'identification et d'authentification offrant un accès universel à l'ensemble des administrations en ligne*[43] ». Plus précisément ce système permet aux usagers du service public français d'accéder à l'ensemble des services publics numériques sans devoir disposer de comptes auprès d'eux. Ce système a été développé fin 2014, expérimenté en 2015 et généralisé en 2016.

C'est la même direction qu'a choisi le Groupe La Poste[44], en créant l'*IDentité Numérique,* permettant de simplifier les formalités sur l'Internet. On note par exemple que les détenteurs de l'*IDentité Numérique* pourront recevoir par courrier électronique des recommandés, se connecter sur des sites Internet *via* leur identifiant et mot de passe *IDentité Numérique*. L'idée est de permettre aux utilisateurs d'obtenir un profil vérifié en ligne sans qu'ils aient à révéler leur véritable identité. Pour cela, il suffit de remplir un formulaire sur Internet et d'attendre le passage du facteur pour la vérification des données déclarées au moment de l'inscription en ligne.

Allant encore plus loin, certains pays avant-gardistes ont opté pour le vote à distance. Ainsi, dans le cadre des élections locales, quelques pays à l'instar de l'Estonie ou du Pérou, ont mis en place un système permettant aux citoyens de voter *via* l'Internet. Il est en effet possible pour les citoyens péruviens de voter *via* une plateforme numérique spécialement dédiée aux élections. L'électeur peut procéder à ce vote grâce à un numéro d'identification personnelle qu'il aura préalablement reçu. Un accusé-réception du vote lui sera transmis sur sa boîte de courriel.

42. *Pour un humanisme numérique*, Paris, Le Seuil, 2011, p. 170.
43. http ://etatplateforme.modernisation.gouv.fr/identite-numerique.
44. https ://www.idn.laposte.fr/discover

Il faut préciser que le droit à une identité numérique comprend deux corolaires : d'une part, l'interdiction de se voir empêcher d'accéder aux réseaux numériques et, d'autre part, la sanction de l'usurpation d'identité. Ces corolaires revêtent une importance accrue depuis que les droits positifs se calquent dans le monde numérique.

C'est au regard de cette (r)évolution des services en ligne et de l'importance du phénomène Internet qu'il semble primordial de consacrer un droit à l'identité numérique. De la reconnaissance même de cette identité numérique découlent des principes fondamentaux qui constituent le cadre juridique des droits de l'homme virtuels, permettant aux individus l'exercice des libertés publiques numériques individuelles et collectives. Cela conduit indubitablement au développement d'une véritable citoyenneté numérique impliquant la liberté d'expression sur la toile, le droit de vote, la liberté associative et syndicale, etc.

9 Conclusion

Le 5 septembre 2000 a eu lieu au siège de l'ONU à New York, l'Assemblée du Millénaire. Ce début de Millénaire avait été perçu comme un moment unique, symbolique et incontournable pour l'ONU afin de réaffirmer sa vision et ses objectifs par le biais notamment de la Déclaration du Millénaire 55/2, adoptée en séance plénière le 8 septembre 2000. Les 189 États membres avaient ainsi décidé « *de faire en sorte que les avantages des nouvelles technologies, en particulier des technologies de l'information et de la communication, soient accordés à tous*[45] ».

Cette Déclaration intervenait opportunément, puisque les années 2000 ont été marquées par l'explosion du domaine des nouvelles technologies de l'information et de la communication. L'Internet a permis de révolutionner le monde à coup de clics et de « like ».

Si le réseau des réseaux ne crée pas toujours de nouvelles difficultés, il en amplifie certaines autres. On constate l'existence d'un fossé numérique entre le Nord et le Sud du globe[46], qu'il est indispensable de combler afin de voir l'émergence d'une société mondiale de l'information. De même, on observe que les infractions de la vie « moléculaire » se sont transposées dans la vie numérique mais aussi que de nouveaux types d'infractions ont vu le jour, et que de nouveaux droits doivent être consacrés.

Il faut intervenir par de nouvelles normes fondamentales afin de permettre un accès plus équitable au réseau et organiser les droits et obligations des internautes.

Cette nouvelle génération de droits de l'homme est certainement une opportunité de recherche sur laquelle l'Institut des droits de l'homme de Lyon (IDHL) pourrait se pencher pendant les trente prochaines années ! Il en a le dynamisme et les compétences. En attendant, qu'il nous soit permis de lui souhaiter un très joyeux anniversaire. Ses « pères fondateurs » peuvent être très fiers de cet « enfant » si brillant !

45. Voir III. Développement et élimination de la pauvreté ; Déclaration du Millénaire 55/2, adoptée en séance plénière le 8 Septembre 2000.

46. Voir allocution d'ouverture de Kofi Annan lors de la réunion de l'Assemblée générale du 17 Juin 2002 sur les technologies de l'information et de la communication au service du développement : http ://www.un.org/press/fr/2002/AG1295.doc.htm