

## INTERNET ET LE DROIT – DE QUELQUES CONSIDÉRATIONS INTRODUCTIVES

Yves POULLET

Professeur facultés de droit de Namur et de Liège

Directeur du CRID Université de Namur (Belgique)

<http://www.crid.be>

[yves.poullet@fundp.ac.be](mailto:yves.poullet@fundp.ac.be)

-----

### Plan de l'intervention<sup>1</sup>

**INTRODUCTION.....3**

**TITRE 1 : LES ACTEURS DE LA RÉGULATION DE L'INTERNET : LA  
GOUVERNANCE DE L'INTERNET.....3**

SOUS TITRE I : DES MODES DE RÉGULATION VARIÉS..... 4

*Section I : L'affirmation de l'autorégulation.....5*

*Section II : La régulation par la technique.....6*

*Section III : Vers un nouveau modèle : la co-régulation.....10*

SOUS-TITRE II : DE LA MONTÉE EN PUISSANCE DES ORGANISATIONS  
SUPRANATIONALES .....11

*Section I : La remise en cause de l'Etat  
souverain.....*

*Section II : La montée en puissance des organisations internationales*  
.....

1. Les organisations globales.....

---

I. La montée des « régionalismes » : un droit européen de l'Internet ?  
.....

A. Créer un marché interne unique .....

B. Les relations avec les pays tiers : de la politique défensive à une politique plus participative .....

**TITRE II : LE CONTENU DE LA RÉGULATION EUROPÉENNE ET INTERNATIONALE DE L'INTERNET QUELQUES TRAITÉS MARQUANTS**  
.....

SOUS-TITRE I: LES OPÉRATIONS : UN CADRE JURIDIQUE POUR LES TRANSACTIONS JURIDIQUES .....

*Section I – Les directives de base.....*

*Section II : En ce qui concerne quelques aspects ou opérations spécifiques*  
.....

SOUS-TITRE II : LES VALEURS : UN DIFFICILE ÉQUILIBRE ENTRE « LIBERTÉS » ET « SÉCURITÉ » DU RÉSEAU. ....

*Section I . Le délicat équilibre entre la liberté d'expression et d'autres intérêts dignes de protection.....*

*Section II. La protection des données à caractère personnel.....*

SOUS-TITRE III. DE LA SECURITE ET DE LA LUTTE CONTRE LA CYBERCRIMINALITE .....

SOUS-TITRE III. DES CONTENUS À PROTÉGER PAR LES DROITS DE PROPRIÉTÉ INTELLECTUELLE ET LES DROITS

VOISINS : DE L'AFFIRMATION AUX DOUTES  
.....

**CONCLUSIONS.....**

## **Introduction**

Entre le droit et la technologie des systèmes d'information, les interactions sont nombreuses. La technologie, dit-on, révolutionne le droit voire en sape les fondements. Ses caractéristiques : la globalisation, la dématérialisation, le caractère distant et interactif, l'absence de toute autorité centrale, heurtent les bases mêmes de l'action réglementaire ou plaident en tout cas pour des modes de régulation nouveaux dont le droit étatique a été écarté dans un premier temps. Son retour progressif s'explique au fur et à mesure que l'Internet devient un fait sociétal majeur et que ses applications envahissent nos entreprises, administrations et foyers et nombre de nos relations interpersonnelles. Tel sera le premier temps de notre réflexion centrée sur les acteurs de la régulation de l'Internet.

Au delà, se concentrant sur l'approche réglementaire internationale et européenne, l'étude propose quelques réflexions sur les objets de la réglementation. Pour faire bref, le droit impose quelques contraintes au développement technologique de manière à sauvegarder, d'une part, les libertés fondatrices de nos sociétés et, d'autre part, les équilibres essentiels inscrits au coeur des législations préexistantes à la société dite de l'Information. Dans le même temps, le droit crée un environnement favorable au développement de cette société. Ce double souci se traduit à travers les nombreuses dispositions spécifiques consacrées aux phénomènes ou développements nouveaux suscités par les technologies de l'information et de la communication.

## **Titre 1. Les acteurs de la régulation de l'Internet : la gouvernance de l'Internet**

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<sup>2</sup>. Là où l'Etat 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

---

<sup>2</sup> 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, pp. 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. Plus récemment, J. BING and L. BYGRAEVE, *Internet Governance*, Oxford University Press, London, 2009.

sans ancrage nécessaire unique dans un territoire donné<sup>3</sup> et surtout sa nature interactive remettent profondément en cause les schémas traditionnels de réglementation fondée sur la souveraineté étatique<sup>4</sup>.

Sous ce titre, notre propos sera dès lors double :

Il s'agira, dans un premier temps, au-delà de la distinction entre les notions de réglementation et de régulation, de rappeler le mythe fondateur de l'Internet, comme espace sans droit, livré aux seules vertus de l'autorégulation et de décrire la montée progressive de systèmes dits de co-régulation ou de « régulation en réseau »<sup>5</sup>.

Le second temps s'attache aux conséquences de la dimension internationale des technologies de l'information et décuplés par les possibilités offertes par l'Internet qui justifient tant l'irruption de nouveaux acteurs, nés de l'autorégulation de l'Internet que la montée en puissance mais quelque peu désordonnée des organisations régionales et internationales.

### **Sous titre I : Des modes de régulation variés**

La création, l'utilisation et le fonctionnement des systèmes d'information ne se conçoivent plus sans leur intégration au sein du réseau mondial ou plutôt du réseau des réseaux que leur ouvrent les protocoles et applications de l'Internet. La régulation de l'Internet s'élabore dès lors dans un contexte doublement délivré des contraintes étatiques à la fois par le fait qu'elle peut se négocier du fait de l'interactivité du réseau<sup>6</sup> et que le phénomène de l'Internet ignore les frontières<sup>7</sup>.

---

<sup>3</sup> Sur ces caractéristiques « dématérialisation », « déterritorialisation », « détemporalisation », lire Th. HOEREN, *Internet und Recht – Neue Paradigm des Informationsrechts*, *NJW*, 1998, vol. 39, p. 2849 et s..

<sup>4</sup> Sur cette approche traditionnelle du droit et sa remise en cause par le phénomène de l'Internet, lire entre autres : Ph. AMBLARD, *Régulation de l'Internet*, Cahier du CRID n° 24, p. 29 et s.; D.R. JOHNSON et DG POST, « Law and Borders – The Rise of Law in Cyberspace », *Stan. L. Rev.*, 1996, vol. 48, p. 1367 et s.

<sup>5</sup> Pour reprendre l'idée centrale de la thèse de OST et VAN DE KERCHOVE, *De la pyramide au réseau ? Pour une théorie dialectique du droit*, Bruxelles, Publ. FUSL, 2002, p. 26. Les auteurs démontrent que de manière générale, le droit a tendance à passer d'un modèle centralisé, hiérarchisé, fondé sur l'Etat nation à un mode d'intervention normative décentralisé, souvent négociée entre auteurs privés et publics, nationaux ou non.

<sup>6</sup> 5 A cet égard, sur cette « contractualisation » du droit de l'Internet, les réflexions déjà anciennes de T. HARDY, « The proper legal regime for Cyberspace », *U. Pitt. L. Rev.*, 1994, vol. 55, p. 999 et s. (spéc. p.1029) ; M. VIVANT, « Internet et modes de régulation », in *Internet face au droit*, Cahier du CRID, n° 12, Bruxelles, Story Scientia, 1997, p. 215 et s.

## Section I : L'affirmation de l'autorégulation

Il était dès lors tentant – et les premiers auteurs du droit de l'Internet<sup>7</sup> ont succombé à cette tentation – de prôner l'abolition de toute réglementation étatique à propos des activités de l'Internet et de prôner une normativité ou régulation livrée aux seules volontés des concepteurs et utilisateurs de l'Internet, soit une « autorégulation »<sup>8</sup>. Ainsi, se sont développées en marge des systèmes juridiques traditionnels, des normativités propres à des communautés virtuelles<sup>9</sup> disposant de leurs propres contenus, modes de contrôles<sup>10</sup>, systèmes de règlements de conflits<sup>11</sup> et de sanctions<sup>12</sup>. Le cas d'e-Bay, sans doute la plateforme ou place de marché Internet la plus populaire, peut être cité en exemple<sup>13</sup>.

À cette autorégulation « contractuelle » née de l'interactivité des réseaux ou secrétée par les usages ou décisions d'acteurs<sup>14</sup> ou de communautés virtuelles,

---

<sup>7</sup> A ce propos, bornons-nous à reprendre les réflexions du grand internationaliste français : J.R. DUPUY, « Nous avons le monde des Etats, qui est celui du cloisonnement. Les pouvoirs s'y répartissent sur des espaces ajustés. De l'autre, nous avons le cybermonde, construit sur un 'écheveau communicationnel' ouvert aux communications et aux échanges et ce sans considération de frontières. », in *Le dédoublement du monde*, RGDIP, 1996, p. 313 et s; Cf. également KW. GREWLICH, *Governance in Cyberspace*, La Haye, Kluwer, 1999, pp. 20-28.

<sup>8</sup> Sur ce concept, lire notamment P. TRUDEL, « Quel droit et quelle régulation dans le cyberspace ? », *Sociologie et Sociétés*, 2000, vol. 32, p. 190 et s. ; plus récemment l'étude très complète de Mr. AMBLARD déjà citée

<sup>9</sup> A propos de cette tendance de l'autorégulation sur Internet à se développer comme un système normatif complet, nos réflexions in « Les diverses techniques de réglementation d'Internet : l'autorégulation et le rôle du droit étatique », *Ubiquité*, 2000, vol. 5, p. 55 et s.

<sup>10</sup> Ainsi, les systèmes de « Hot lines » et de « labels » de qualité des sites Internet mis en place spontanément par le marché. Sur la labellisation des sites web, lire entre autres O. CACHARD, *La régulation internationale du marché électronique*, Paris, LGDJ, 2002, p. 270 et s.

<sup>11</sup> Ce qu'il est convenu d'appeler les Online Dispute Resolution Mechanisms » (ODR). Sur ces ODR, lire l'analyse critique de ceux-ci, par Mr. Th. SCHULTZ (op.cit) et la description des différents ODR mis en place par G. KAUFMANN-KOHLER et T. SCHULTZ, *Online Dispute Resolution : Challenges for Contemporary Justice*, La Haye, Kluwer, 2004.

<sup>12</sup> On évoque les « systèmes de gestion de réputation » qui permettent aux internautes de mieux connaître l'opinion de ses collègues à propos d'un site, les « listes noires » ou le retrait de labels ou l'exclusion des places de marché.

<sup>13</sup> A cet égard, la très belle étude de T. SCHULTZ, XXX. Sur ce cas, lire également, E. KATSCH, J. RIFKIN et A. GATTENBY, « E-commerce, E-dispute, and E-Dispute Resolution : in the Shadow of « e-Bay Law », *Ohio St. J. on Disp. Resol.*, 2000, vol. 15, p. 705 et s.

<sup>14</sup> Ainsi, d'innombrables « Privacy Policies » ou « Conditions (Terms) of Use » présentes sur les sites de l'Internet.

s'ajoute celle dictée par la technique elle-même<sup>15</sup>. Le vocable de « Lex electronica » ou « Lex informatica », héritière de la « Lex mercatoria »<sup>16</sup>, largement développé par des auteurs comme L. LESSIG<sup>17</sup> et J. REIDENBERG<sup>18</sup> entend précisément que les choix opérés au niveau de l'infrastructure peuvent déterminer les usages de l'Internet et constituent donc une forme de régulation<sup>19</sup>.

## Section II : La régulation par la technique

Dans un article publié en 1993, J. Reidenberg<sup>20</sup> soulignait déjà le hiatus entre deux mondes: celui de la réglementation des opérations et celui de la normalisation technique. Le premier monde ressortait indiscutablement de la compétence des législateurs nationaux traditionnels, simplement l'ampleur des questions nécessitant de plus en plus de coopérations au sein des organisations internationales ou régionales. Le second monde émergeait à l'époque : la normalisation d'une infrastructure globale comme celle d'Internet exigeait des décisions qui ne pouvaient être prises qu'au sein des organes dits de régulation technique aux compétences encore balbutiantes, organes que les pionniers d'Internet avaient mis au point<sup>21</sup>.

---

<sup>15</sup> Pour une application de cette multi régulation aux cas des plateformes du Web 2.0, lire l'article de P. TRUDEL, La régulation du Web 2.0, *RDTI*, 2008, pp. 284 à 307

<sup>16</sup> Pour une histoire de la norme et la fausse comparaison entre la « Lex mercatoria » et la « Lex electronica », lire les développements de K. BENYEKLEEF, *Histoire de la norme*, Thémis, Montréal, 2008.

<sup>17</sup> « Une idée définit la pensée de la première génération au sujet de cet espace. Le cyberspace, disait-on, ne peut pas être régulé. Il ne 'peut pas être gouverné', il a une habileté innée à résister à la régulation. C'est là sa nature, son essence, c'est ainsi que sont les choses (...). Le cyberspace est un espace de non contrôle », L. LESSIG, *Code and other Laws of Cyberspace*, New York, Basic Books, 1999, p. 24; Comp. Negroponte (Being Digital, New York, Vintage Books, 1995, p. 237 : «(Le droit est) un poisson mourant sur les quais, parcouru de spasmes, tentant de happer une dernière bouffée d'air, en vain, car le monde numérique est un lieu différent ».

<sup>18</sup> Surtout, J. REIDENBERG, « Lex Informatica : The Formulation of Information Policy Rules Through Technology », *Tex. L. Rev.*, 1998, vol. 76, p. 553 et s.

<sup>19</sup> On citera la célèbre affirmation de cet auteur : « Code is the law » (*Code and other Laws of Cyberspace*, op. cit.). Du même auteur, on lira : « The Constitution of Code : Limitations on Choice and critiques of Cyberspace Regulation », *Comm. Law Conspectus*, 1997, vol. 5, p. 181 et s. et «The Law of the Horse : What Cyberlaw Might Teach», *Harw. L. Rev.*, 1999, vol. 113, p. 501 et s.. Dans le meme sens, C. ROJINSKY, « Cyberspace et nouvelles régulations technologiques », *D.*, 2001, Chron., p. 844 et s. Pour une vision très critique de cette affirmation, G. GREENLEAF, « An End-note on Regulating in Cyberspace : Architecture v.Law », *UNSW Law Journal*, 1998, vol. 21, p. 593 et s.

<sup>20</sup> J. REIDENBERG, Du même auteur, on notera les articles parus depuis: "Governing Networks and Rules- Making in Cyberspace, *45 Emory Law Journal*, 1996, 912-930 ; "Lex Infomatica : The Formulation of Information Policy Rules through Technology", *76, Texas Law Review*, 1998, 553-593.

<sup>21</sup> Sur ces différents organes de normalisation technique en matière de technologies de l'information et de la communication, lire J. BING et L. BYGRAEVE, *op. cit.*, p. 92 à 146. P. TRUDEL (ed.), *Droit du cyberspace*, Montréal, Thémis, 1997 ; J. BERLEUR, Y.POULLET, « Quelles régulations pour l'Internet », in *Gouvernance de la société de l'information*, Cahier du CRID n° 22, Bruxelles, Bruylant, p. 133 et s.

Ces organes, comme l'IETF<sup>22</sup>, le W3C<sup>23</sup>, l'IANA devenue l'ICANN<sup>24</sup>, ont en même temps qu'Internet tissait sa toile, acquis, sans renier leur statut d'origine, leurs lettres de noblesse parfois avec la complicité de gouvernements<sup>25</sup> ou d'organisations internationales<sup>26</sup>. Qui ne comprend qu'au-delà d'une normalisation technique, comme l'attribution de noms de domaines<sup>27</sup>, l'adressage d'Internet, le « design » de l'infrastructure, la définition de protocoles techniques de filtrage des contenus, etc., il s'agit de décisions dont le contenu en un autre temps eût été pris par des auteurs, objet d'une légitimité constitutionnelle<sup>28</sup>. La même tendance à confier la gouvernance de technologies nouvelles à des organisations privées existe en matière de Radio Frequency Identifiers (RFID) où très rapidement les acteurs du

---

<sup>22</sup> Sur l'Internet Engineering Task Force (I.E.T.F), lire M. A. FROOMKIN, "Habermas @discourse net : Toward a critical theory of cyberspace", *116 Harv. Law Rev.*, p. 800 et s (2003) ; S. BRADNER, "IETF Working Group Guidelines and Procedures", disponible sur le site : <http://www.ietf.org/rfc>.

<sup>23</sup> À propos du W3C qui contrôle le développement du HTML et des autres standards du Web, lire S.L. GARFINKEL, « The Web's Government », *MIT Technology Review*, 38.46 (Nov.- Déc. 98) disponible sur le site de l'IETF. Le lecteur visitera le site du W3C : <http://www.w3c.org.consortium>

<sup>24</sup> Sur l'histoire de l'ICANN, J. WEINBERG, "ICANN and the problem of legitimacy". *50, Duke Journal*, 187 (2000).

<sup>25</sup> À cet égard, à propos du soutien du Département of Commerce américain à la création de l'ICANN et de la volonté du gouvernement américain de garder par l'ICANN le contrôle de la gouvernance de l'Internet, lire les articles de M. FROOMKIN « Wrong Turn in Cyberspace : Using ICANN to Route Around the APA and the Constitution », *50 Duke, L.J.* 17 (2000) et « Form and Substance in Cyberspace », *Northwestern and School of Law of Lewis & Clark College*, 93 et s. (2002). coup génial du point de vue américain face au monde d'Al gore : commercialiser internet = un basculement total, techniques développées sur contrats militaires américains (Darpa) dans le milieu de la recherche étendu sans aucune considération sur le fait que « la société » ne fonctionne pas comme le milieu protégé de la recherche, et contre l'IUT qui régissait jusque là les normes de télécommunications

<sup>26</sup> Ainsi les liens entre l'OMPI et l'ICANN lors de la rédaction des fameuses UDRP (Uniform Dispute Resolution Procedure) en matière de noms de domaines où c'est l'OMPI organisation publique qui a rédigé pour le compte de l'ICANN les règles procédurales en matière de conflits portant sur des noms de domaine. Par contre, le combat en 1992 entre l'IETF et l'UIT sur le choix entre le protocole TCP IP et le modèle en couches OSI a tourné au bénéfice du premier nommé..

<sup>27</sup> Ainsi, la question de l'attribution de domaines pose des questions de droit de propriété intellectuelle, la création du *Whois* soulève des questions de protection de la vie privée. Plus grave, le choix des noms génériques et l'attribution de noms de domaines à certaines nations comme le Palestine soulève des questions de respect des Etats ? Sur l'impossibilité de distinguer questions techniques et questions de société, le remarquable article de J. REIDENBERG, "Lex Informatica : The formulation of Information Policy Rules in Techology", *76, Texas Law Review*, 1998, 553-584; et l'ouvrage de base de L. LESSIG, *Code and Other Laws of Cyberspace*, op.cit.

<sup>28</sup> À propos de la légitimité contestable des organes de normalisation technique, lire AM FROOMKIN, « Habermas @discourse net : Toward a critical theory of cyberspace », *116 Harv. Law Rev.*, p. 751 et s (2003) ; Sur cette émergence des "pouvoirs" privés et leur rôle réglementaire, lire F. OST et M. van DE KERCKOVE, « De la pyramide au réseau ? Vers un nouveau mode de production du droit », *Rev. Interdiscipl. d'études juridiques*, 2000, 44, pp. 66 et s.

terrain ont mis sur pied une organisation, l' « Electronic Product Code » (EPC) association pour décider des normes d'attribution et de fonctionnement en la matière<sup>29</sup>. Une telle assertion est à la base même de l'ouvrage qui, sans aucun doute, a le plus marqué la littérature juridique voire l'opinion publique sur les relations entre droit et technologie : « Code and other Laws of Cyberspace » de Lawrence LESSIG<sup>27</sup>. Selon LESSIG, l'architecture technique, les caractéristiques du réseau (les protocoles, les standards de communications retenus, ...) créent un environnement autorisant certains comportements et en interdisant d'autres et jouent donc un rôle essentiel dans la régulation du cyberspace. Par ailleurs, il est remarquable de constater que les législateurs et juges devront tenir compte de ce donné décidé ailleurs que dans les enceintes traditionnelles du droit<sup>30</sup>.

Celle-ci échappe largement aux Etats : « L'élaboration (des normes mises en oeuvre par la technique), écrit REIDENBERG, ne dépend pas de la participation de tous les acteurs de l'Internet. Ce sont les spécialistes seuls qui décident des règles (...). Les techniciens choisissent la mise en oeuvre des protocoles techniques. Les citoyens à qui des règles s'appliquent ne participent pas de façon directe à leur développement ». « Tandis que les Etats continuent à se demander quel type de réglementation devrait être adoptée, poursuit L. LESSIG<sup>31</sup>, le code du cyberspace continue à se développer avec quelque chose qui ressemble à une autorité souveraine ». Nous reviendrons plus loin sur les acteurs de cette gouvernance technique de l'Internet.

Si notre propos n'est pas de reprendre ici des réflexions proposées ailleurs<sup>32</sup> sur les relations entre « Droit et Technologie », relevons cependant à ce propos de

---

<sup>29</sup> Sur cette organisation privée mondiale, lire Y. POULLET, D. DARQUENNES, « RFID quelques réflexions introductives à un débat de société », dans *R.D.T.I.*, 2006, n° 26, pp. 255-285.

<sup>30</sup> L. LESSIG, *Code and Other Laws of Cyberspace*, op.cit. (disponible sur le site : <http://www.cyberlawstanford.edu.lessig.content.index.htm>) Selon LESSIG, la régulation d'Internet résulte de l'interaction de quatre modes de régulation : la loi, les normes sociales, leur marché et surtout l'architecture technique

<sup>31</sup> L. LESSIG, *Code and Other Laws of Cyberspace*, op.cit. (disponible sur le site : <http://www.cyberlawstanford.edu.lessig.content.index.htm>)

<sup>32</sup> Y. POULLET, « La technologie et le droit, Du défi à l'alliance », in *La technologie et le droit : du défi à l'alliance*, Liber Amicorum Guy HORSMANS, Bruylant, 2004, p. 943 et s.. Cf. également, de manière très générale, S. GUTWIRTH, *Waarheidsaanspraken In Recht en wetenschap*, Maklu, Antwerpen, 1993. Sur l'interaction entre la régulation technique de l'Internet et la régulation traditionnelle, lire J. REIDENBERG, « Privacy Protection and the Interdependence of Law, Technology and Self-Regulation », in *Variations sur le droit de la société de l'information*, Cahier du CRID, n° 20, pp. 130 et s.; Y. POULLET, « How to regulate Internet, New Paradigm for Internet Governance », publié dans le même ouvrage, pp. 79 et s.

cette interaction : Droit et Technologie, deux éléments pointés à partir de deux domaines distincts du développement technologique.

- Le premier est celui des systèmes techniques permettant de protéger l'accès aux ressources informationnelles présentes sur le Net, de limiter ou d'interdire les copies, voire le cas échéant, d'assurer la traçabilité de leur utilisation au sein du réseau. Ces systèmes techniques dits de gestion des droits<sup>33</sup> renforcent les protections juridiques des auteurs voire les rendent inutiles dans la mesure où la technologie assure une protection bien plus efficace et plus absolue des intérêts des concepteurs d'une « oeuvre » qu'elle soit digne ou non de protection par le droit d'auteur<sup>34</sup>. Ainsi, la technique ou, plutôt, les choix technologiques opérés par ceux qui les promeuvent et auxquels peuvent être liées des coalitions d'intérêts politico-économiques, peuvent au-delà de la protection des droits modifier profondément les équilibres inscrits au cœur de leur reconnaissance voire rendre inutile la proclamation de ces droits.

Le second exemple est tiré des standards PICS<sup>35</sup> ou P3P<sup>36</sup>, développés tous deux par le W3C., organe privé de normalisation technique des applications liées aux protocoles html. Des logiciels construits sur base de ces standards peuvent être introduits dans le navigateur de l'internaute ou mis à sa disposition par des fournisseurs de services. Grâce aux paramétrages qui caractérisent ces logiciels, l'Internaute peut fixer, tantôt dans le cas des PICS, les critères de qualité des contenus des sites web à sélectionner et cela, selon la violence, le langage ou le

---

<sup>33</sup> 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, Janv. 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.

<sup>34</sup> C'est toute la thèse de S. DUSOLLIER, *La protection appropriée des mesures techniques en droit d'auteur*, Larcier, Bruxelles, 2005. Cf. également, T. VINJE, "A brave new world of technical Protection Systems. Will there still be a room for Copyright", *EIPR*, 1996, n° 8, p. 431. Un autre exemple en matière de droit de la propriété intellectuelle est donné par V. BENABOU lorsqu'elle démontre que le tatouage des œuvres qui permet la protection de chaque élément de l'œuvre va bien au-delà de la protection que le droit d'auteur assure à l'œuvre prise comme un tout (V. BENABOU, « L'œuvre poulpe », *RDTI*, 2009, p. 312.

<sup>35</sup> Platform for Internet Content Selection. Le lecteur trouvera une bonne description des PICS in R.P. WAGNER, "Filters and the First Amendment", *83 Minn. L. Rev.* (1998), p. 755 et s.

<sup>36</sup> Platform for Privacy Preferences. Le lecteur trouvera une description de son fonctionnement in L.F. CRANOR, "Agents of Choice : Tools that facilitate Notice and Choice about Web Site Data Practices", texte disponible sur le site <http://www.research.ATT.com/~lorrie/pubs/hk.pdf>. Les « *privacy settings* » mises à la disposition d'un réseau social comme Facebook, permettant à l'utilisateur de Facebook de limiter le nombre d'« amis » autorisés à accéder aux informations mises par l'utilisateur sur ses pages Facebook répond à la même idée d'un outil technologique permettant à l'internaute de réguler lui-même ses relations avec autrui.

caractère sexuel de ces sites, tantôt dans le cas du P.3.P., les exigences de vie privée à respecter par ces mêmes sites. La technologie offre ainsi la possibilité pour l'Internaute de réguler lui-même son environnement et crée ainsi l'illusion d'un « *User Empowerment* »<sup>37</sup>.

### **Section III : Vers un nouveau modèle : la corégulation**

Dans la mesure où l'Internet est devenu un fait sociétal majeur, pénétrant au-delà de nos entreprises, nos administrations et nos foyers et nos relations interpersonnelles dans la mesure où il met en jeu des valeurs éthiques et culturelles auxquelles les nations sont attachées, et, surtout, exige pour son développement, la confiance, le modèle de l'autorégulation a progressivement montré ses limites. L'Etat est rappelé en force, d'une part, pour affirmer ses valeurs ou, après le 11 septembre noir, les impératifs de la sécurité publique<sup>38</sup>, et d'autre part, pour créer le cadre de confiance et de sécurité juridique nécessaire pour un développement de l'économie basé sur le commerce électronique<sup>39</sup>.

Cette « renaissance » du pouvoir étatique ne se conçoit cependant pas comme une affirmation brutale de l'autorité étatique. Elle se conçoit comme une « coopération entre la société civile et les pouvoirs publics<sup>40</sup> », un « effective mix »<sup>41</sup>,

---

<sup>37</sup> A propos de cette notion et de la critique qu'il convient de lui adresser, Y. POULLET, M. D'UDEKEM-GEVERS, « Internet content regulation: concerns from a European user empowerment perspective about Internet content regulation : An analysis of some recent statements », Part I, *C.L.S.R.*, 2001, Vol. 17, n° 6, pp. 371-377; Part II, *C.L.S.R.*, 2002, Vol. 18, n° 1, pp. 11-23.

<sup>38</sup> À propos de cette renaissance des « souverainetés étatiques » et la notion de « frontières virtuelles » défendue par le gouvernement américain, lire J. REIDENBERG, « States and Internet Enforcement », *Univ. Ottawa L & Tech.J.*, 2004, disponible sur le site : <http://www.srn.com/abstract=487965>. Cette notion justifie notamment l'obligation faite aux transporteurs aériens par l'administration américaine de permettre l'accès aux données des passagers. Sur le dossier « Passenger Name Record », lire Y. POULLET – V. PEREZ-ASINARI, « *Données des voyageurs aériens : le débat Europe- Etats -Unis* », *J.T.D.E.*, 2004, p. 266 et s.

<sup>39</sup> Sur la renaissance de la loi dictée par la nécessité de créer un cadre de confiance, lire J. BERLEUR - Y. POULLET, « Réguler Internet », *Revue Etudes*, 2002, vol. 397, n° 5, p. 470-471 : « Comment expliquer ce phénomène ? Un seul mot, nous l'avons déjà dit : la confiance. Que la loi ait une fonction rassurante est indéniable. Elle crée un cadre de référence, soumet les acteurs à des prescrits qui garantissent la sécurité, la loyauté et la bonne fin des opérations ».

<sup>40</sup> Selon la définition donnée par le rapport de C. PAUL, *Du droit et des libertés sur l'Internet, La corégulation, contribution française pour une régulation mondiale*, Rapport au Premier Ministre, Paris, La Documentation française, 2000, n° 141, Supplément, p. 9.

<sup>41</sup> Selon la définition donnée par l'OCDE à la corégulation. Sur l'historique de la corégulation, la notion et ses diverses formes, lire Y. POULLET, « Technologies de l'information et de la communication et 'corégulation' : une nouvelle approche ? », in *Liber Amicorum M. COIPEL*, Kluwer, Antwerpen, 2004, p. xxx

ou, tantôt, l'Etat consolide des processus d'auto-régulation mis en place par le secteur privé lui-même<sup>42</sup> ; tantôt, après avoir fixé législativement les objectifs à poursuivre, l'Etat laisse à des instances de consultation<sup>43</sup> ou aux acteurs privés le soin de traduire les « standards » mis en place par ses lois<sup>44</sup>. Cette multiplication sous diverses modalités des formes de coopération entre réglementations voire régulation publique et régulation privée dans le domaine de la régulation de l'Internet est largement prônée par les « Sommets mondiaux de la Société de l'information », initiative des Nations-Unies dans le cadre de la déclaration du millénaire, tenus à Genève et Tunis et Prolongés par les Forums de la Gouvernance de l'Internet. Nous reviendrons dans le point suivant sur les conclusions majeures de ces Sommets.

## **Sous-titre II : De la montée en puissance des organisations supranationales**

Le caractère « sans frontières » de l'infrastructure de l'Internet, la globalisation des activités que l'Internet permet remettent en cause la possibilité pour les Etats nations d'exercer pleinement leur souveraineté (Section I).

A partir de ce contexte, on soulignera :

- La volonté de créer ou renforcer des régulateurs « globaux ». À cet égard, nous reviendrons sur l'intervention déjà signalée des organes privés de normalisation technique et sur celle croissante des organisations publiques internationales (Section II) ;
- Entre ces institutions globales et les Etats nations, la montée en puissance des organes supranationaux régionaux.. Notre propos sur ce point se limitera à quelques considérations sur l'action de l'Union européenne, cherchant à la fois à définir un

---

<sup>42</sup> On citera ainsi, les systèmes d'agrément volontaire des labels, la définition de « Best Practices » par des organes officiels ou créés par des instances officielles, ainsi l'e-confidence Forum créé par la Commission européenne (Sur ce forum et ses activités, cf. le site <http://www.jrc.it> ) chargé d'analyser avec les promoteurs et leurs utilisations différents produits de l'autorégulation (code de conduite, labels, ODR, ...).

<sup>43</sup> Ainsi les « autorités de contrôle » en matière de vie privée, les autorités administratives indépendantes en matière de réglementation de l'audiovisuel et de télécommunication, les observatoires de droit de l' Internet ou autres commissions « télématique », etc..

<sup>44</sup> En ajoutant par cette traduction, une certaine « valeur ajoutée ». Sur cette notion et sa signification dans divers documents européens, lire Y. POULLET, « Vers la confiance : vue de Bruxelles : un droit européen de l'Internet ? Quelques considérations sur la spécificité de l'approche réglementaire européenne », Bull. d'actualités, *Lamy Droit de l'Informatique et des réseaux*, 2001, n° 141.

droit européen harmonisé de l'Internet et à proposer son modèle vis-à-vis d'autres modèles, en particulier celui des Etats Unis (Section III).

## Section I : La remise en cause de l'Etat souverain

L'Etat national exerçait dans le cadre de son territoire, sa souveraineté<sup>45</sup>. La technologie remet en cause cette « souveraineté » à plus d'un titre.

Premièrement, la dématérialisation des investissements principalement immatériels que représente l'économie de l'Internet permet facilement la délocalisation de ces investissements et, l'Etat nation a le choix entre, d'une part, des stratégies d'isolement, ou de dumping réglementaires qui risquent de se retourner contre lui, et, d'autre part, la recherche d'une harmonisation des législations. Cette seconde solution sera préférée<sup>46</sup>.

Deuxièmement, l'abolition des frontières rend dérisoire la « prétention des Etats à régenter le net ». Ainsi, note Vivant<sup>47</sup>, il y a « contradiction entre un phénomène qui ignore les frontières et des entités qui n'existent et n'ont compétence qu'à l'intérieur de frontières données ».

Troisièmement, si les règles de droit international privé permettent encore aux tribunaux d'affirmer la prééminence des lois nationales, les solutions prônées peuvent être combattues par des juridictions étrangères et en toute hypothèse, la décision se heurtera à l'impossibilité d'en assurer l'application dans le cadre d'un réseau sans frontières. L'affaire Yahoo illustre à suffisance la vérité du propos<sup>48</sup>.

---

<sup>45</sup> Sur les liens entre « territorialité et Etat » et leur remise en cause par l'émergence de l'immatériel, lire H. RUIZ FABRI, Immatériel, territorialité et Etat, *Arch. Phil. Droit*, T. 43, 1999, pp. 187-212 : « Le développement des communications immatérielles et la poursuite de l'Etat à leurs mouvements posent la question de la maîtrise de l'Etat d'un espace normatif national normalement calqué sur le territoire et exprimé dans le principe de territorialité ». Cf. également GF. CONSTANTIN, « L'informel internationalisé ou la subversion de la territorialité » in B. BADIE et M.C. SMOUTS (éd.), *L'international sans frontières, Cultures et conflits*, n° 21/22, 1996, p. 311-345.

<sup>46</sup> Sur cette préférence fondée sur des arguments d'analyse économique du droit, lire D.L. BURK, « Virtual Exit in the Global Information Economy », *73 Chicago Kent L. Rev.*, 1999, n° 4, p. 970.

<sup>47</sup> M. VIVANT, « Internet et modes de régulation » in *Internet face au droit*, E. Montero (ed.), Cahier du CRID, n° 16, Bruxelles, Story Scientia, p. 226 et s. Cf. également, DR. JOHNSON et DG POST, « Law and Borders – The Rise of Law in Cyberspace », *Stan. L. Rev.*, 1996, vol. 48, p. 2370.

<sup>48</sup> L'affaire Yahoo (UEJF et LICRA c. Yahoo Int., TGI Paris, Ord. Réf. 22 mai 2000, 11 août 2000, 20 nov. 2000, disponible sur : <http://www.legalis.net>), concernait l'accès par des internautes français à des sites d'enchères d'objets nazis accessibles via le portail d'Yahoo. Sur cette affaire, lire J.R. REIDENBERG, « Yahoo and Democracy on the Internet », *Jurimetrics*, J. 2002, vol ; 42, p. 261 et s ; Y. POULLET, « L'affaire Yahoo ou la revanche du droit sur la technologie ? », *Ubiquité*, 2001, vol. 9, p. 81 et s. On note que dans cette affaire Yahoo, l'histoire ne s'arrête pas là et au refus du droit... l'intérêt économique est de nature à prendre le relais. Si la décision française n'a pu être exécutée, Yahoo a cependant modifié ses « Terms of Use » (autorégulation),

Bref, dans cet espace sans frontières où toute information en définitive relève par son ubiquité des juridictions de tous les pays<sup>49</sup>, il faut bien reconnaître que le droit n'apporte plus la sécurité juridique<sup>50</sup>.

## Section II : La montée en puissance des organisations internationales

Que la réponse adéquate à un phénomène de globalisation soit à trouver au niveau d'organisations globales, apparaît évident.

À propos de la régulation des infrastructures et des protocoles qui permettent d'assurer l'interopérabilité de l'ensemble des applications fonctionnant sur le réseau, nous avons déjà (Sous titre 1) noté le rôle d'instances privées de normalisation technique. L'IAB et IETF, les deux organes de régulation technique du réseau créèrent en 1992 l'Internet Society (ISOC)<sup>51</sup>. Quelques temps plus tard, en octobre 1994, avec l'invention du Web, apparaît le World Wide Web Consortium (W3C). Enfin, en décembre 1998, l'Internet Assigned Numbers Authority (IANA), sous tutelle de l'administration américaine était remplacée par l'Internet Corporation for Assigned Names and Numbers (ICANN), une « non profit corporation ».

Ces trois principales organisations privées<sup>52</sup>, bien que n'ayant que des compétences techniques détiennent un pouvoir normatif important. Ils gèrent les ressources rares de l'Internet (adresses, noms de domaines,..). Ils déterminent les spécificités techniques du réseau qui s'imposent à toutes activités régulatrices. Les

---

pour ne pas se couper de tout le marché européen, de modifier ses règles commerciales pour pouvoir refuser un commerçant sur sa plateforme (après la France, en effet, l'Allemagne allait attaquer Yahoo)

<sup>49</sup> P.S. BERMAN, "The Globalization of Jurisdiction", *U.Pa.L. Rev.*, 2002, Vol. 151, p. 311 et s.; M.GEIST, "Is There a There ? Towards Greater Certainty for Internet Jurisdiction", *Berkeley Tech. L. J.*, 2001, vol. 16, p. 134 et s.

<sup>50</sup> Sur ce point, la conclusion de Mme Goyard Fahre (« Les fondements de la légalité », in *Les figures de la légalité*, C.A. MORAND (ed.), Published, Paris, 1992, p. 39) : « (Avec l'Internet), l'instabilité de la loi porte atteinte à sa vocation d'ordre ». Cf. également M. VIVANT, « Cybermonde : droit et droits des réseaux », *JCP,G*, 1996, I, 3969, p. 407.

<sup>51</sup> La création de l'Internet Society (ISOC) a été annoncée en juin 1991 par l'IAB et l'IETF, lors de leur conférence annuelle INET 91 à Copenhague. Mais l'ISOC n'a été officiellement formée qu'en Janvier 1992. Pour plus de précisions ; V. CERF, « IETF and ISOC », <http://www.isoc.org/history/ietfhis.html> Sur l'historique de ces « *Governors of the Internet* », lire l'ouvrage édité sous la direction de L. BYGRAEVE et J. BING, *Internet Governance*, Oxford University., London, 2009 (en particulier les pages 92 à 126) et els nombreuses références.

<sup>52</sup> Ph. AMBLARD, op. cit., p. 72.

règles de conduite relatives à l'Internet ne sont efficaces que si elles se conforment aux caractéristiques techniques du réseau. Mais plus que ce cadre, les organisations peuvent également être une source normative, dans le sens où elles deviennent une technique de direction des conduites des internautes<sup>53</sup>.

## 1. Les organisations globales

Sans doute, serait-il fastidieux de reprendre ici la longue liste des activités des organisations intergouvernementales oeuvrant dans le domaine de la régulation de l'Internet<sup>54</sup>.

Les compétences traditionnelles de l'UNESCO pour le développement de la science, de la culture et de l'éducation ont trouvé à s'appliquer à de nombreuses reprises en matière de technologies de l'information et de la communication<sup>55</sup>.

L'organisation internationale de normalisation (ISO) s'occupe de normalisation technique y compris en matière de système d'information. Elles développent grâce à un groupe technique le JTC 1 pour les technologies de l'information et de la communication des normes volontaires en matière de produits, de services ICT y compris leur sécurité (voir en particulier l'ISO/IEC 27002 définissant un « *Code of Practice* » pour la gestion de la sécurité des systèmes d'information). Ensuite, l'Organisation Mondiale du Commerce (OMC) veille au libre échange en matière de commerce international et donc de commerce électronique et certains accords pris en son sein visent les services et produits de communication. Par ailleurs, dès 1994, l'OMC parvenait à un « Accord sur les aspects des droits de propriété intellectuelle qui touche au commerce » (Accords dits ADPIC) dont certains articles visent la protection des programmes d'ordinateur. Une

---

<sup>53</sup> Pour un aperçu, le lecteur se réfèrera à l'ouvrage de P. TRUDEL et alii, *Droit du cyberspace*, Montréal, Ed. Thémis, 1997, plus particulièrement le Chapitre VI et au rapport établi par l'OCDE à l'occasion de la conférence Ministérielle d'Ottawa (1998) « *Un monde sans frontières : réaliser le potentiel d'un commerce électronique global* », rapport intitulé « Report on international and regional Bodies : Activities and Initiatives in Electronic Commerce », (SG/EC (98) 10/REV2).

<sup>54</sup> Pour un aperçu, le lecteur se réfèrera à l'ouvrage de P. TRUDEL et alii, *Droit du cyberspace*, Montréal, Ed. Thémis, 1997, plus particulièrement le Chapitre VI et au rapport établi par l'OCDE à l'occasion de la conférence Ministérielle d'Ottawa (1998) « *Un monde sans frontières : réaliser le potentiel d'un commerce électronique global* », rapport intitulé « Report on international and regional Bodies : Activities and Initiatives in Electronic Commerce », (SG/EC (98) 10/REV2).

<sup>55</sup> On cite en particulier les recommandations sur la promotion et l'usage du multilinguisme et l'accès universel au cyberspace (2003) disponible sur le site de l'UNESCO. .

décision récente<sup>56</sup> en matière de jeux en ligne opposant Antigua et les Etats-Unis rappellent le droit des Etats de mettre des barrières à l'accès à des services Internet lorsque ceux-ci soulèvent des objections d'ordre public (y compris la vie privée<sup>57</sup>) et de bonnes mœurs pour le pays destinataires des services Une autre institution spécialisée des Nations Unies, la Commission des Nations Unies (CNUDCI) pour le droit du commerce international a produit de nombreuses lois modèles en matière de commerce électronique (Loi modèle sur la signature électronique (2001), Loi modèle sur le commerce électronique (1996), Convention des Nations-Unies sur l'utilisation de communications électroniques dans la passation de transactions internationales (2005).

On citera également le rôle du G8 et de l'OCDE, ce dernier étant particulièrement actif dans les domaines de la protection des données (Lignes directrices de 1980), de la criminalité informatique (Lignes directrices sur la sécurité des systèmes d'information (1992), la taxation des opérations du commerce électronique (Conditions cadre de taxation, 1998) et la protection du consommateur (Orientations relatives aux politiques à mener visant à protéger et à renforcer l'autonomie des consommateurs dans les communications électroniques (1999) et plus récemment Orientations en matière de lutte contre les vols d'identité (2008)) .

- Les compétences de ces diverses organisations dites spécialisées se chevauchent. Ainsi, les questions de la propriété intellectuelle ressortent indiscutablement des compétences de l'OMPI mais ont également été abordées par l'OMC voire par l'UNESCO ;

-Les méthodes utilisées par des organisations relèvent le plus souvent de la « *soft law* »<sup>58</sup> c'est-à-dire consistent en des lois dites « modèles »<sup>59</sup>, des

---

<sup>56</sup> Sur cette décision de l'Appellate Body (2005), M.V. PEREZ-ASINARI, When GATS rules are not applied due to the « Public morals »/ « Public order » exception, CL&SR, 2006, p. XXX.

<sup>57</sup> L'article XIV des accords du Gats de 94 rend légal le refus d'accès au marché au titre de la protection des données personnelles

<sup>58</sup> Également qualifié de « droit souple ». A ce propos, C. THIBIERGE, « Le droit souple », *R.T.D.civ.*, 2003, p. 626 et s. ou J. CHEVALLIER, « Vers un droit postmoderne », in *Les transformations de la régulation juridique*, LGDJ, 1998, p. 21 et s. Cet auteur souligne : « la transformation profonde de la nature du droit dont la dimension proprement normative, prescriptive et contraignante régresse ».

<sup>59</sup> Ainsi, la loi type de la Commission des Nations Unies pour le droit du commerce international (CNUDCI) sur le commerce électronique (6 Déc. 1996).

recommandations<sup>60</sup>; la définition de « Best Practices »<sup>61</sup> voire simplement en des collaborations de ces organisations intergouvernementales avec des organisations privées de régulation. On cite à cet égard, le rôle de l'OMPI dans l'élaboration des « *Uniform Disputes Resolution Procedures* » en matière de noms de domaines, adoptées par l'ICANN<sup>62</sup> ;

Enfin, on pointe la volonté d'instaurer une Constitution globale de la société de l'information, Constitution qui définirait les valeurs fondamentales de cette société et fixerait les règles tant d'un accès universel à cette société, que de son développement dans le respect du multiculturalisme. C'est l'ambition que l'UIT (bien tardivement, dirons certains), forte du mandat des Nations Unies, s'est donné à travers les sommets mondiaux de la société de l'Information, les sommets de Genève et de Tunis<sup>63</sup>. la portée de ces textes, d'une part, universels puisque portés par les Nations Unies et voulus pour consacrer l'Internet comme une « ressource publique mondiale », d'autre part, constituants par la solennité du discours : « Nous, peuples du monde entier,... » et par l'affirmation de trois principes majeurs appelés à gouverner la société de l'Information.

Ces trois principes doivent être rappelés. Le premier proclame la nécessité d'un service public informationnel comme moyen indispensable du développement d'une société de l'information où chacun au-delà de toutes les inégalités puisse accéder aux ressources de l'Internet et contribuer pleinement à la création de savoirs. Sans doute, se plaindra - t'on avec les pays du sud que cette proclamation ne s'accompagne point d'engagements financiers à la hauteur. Le deuxième insiste sur la nécessité d'un développement à la fois multiculturel (« La diversité culturelle est

---

<sup>60</sup> Cf. en particulier, les déclarations ou lignes directrices de l'OCDE en matière de vie privée , Lignes Directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel (1980) ou de sécurité informatique, Lignes directrices régissant la sécurité des systèmes d'information, Nov. 1992.

<sup>61</sup> Ainsi, les « Best Practices » définies par l'UDRP (Uniform Domain Name Dispute Resolution Policy) adoptée par l'ICANN.

<sup>62</sup> Sur cette collaboration, ses modalités et les critiques à apporter à de telles pratiques, lire M.A. FROOMKIN, « Semi private international Rules », in *Regulating the GII*, C. MARDEN (ed.), Frontledge, Londres-New York, 2000, p. 211 et s.

<sup>63</sup> Cf. à ce propos, la Déclaration de principe : « Construire la société de l'information : un défi mondial pour le nouveau millénaire », Genève, 10 déc. 2003 et l'Agenda de Tunis, Tunis 2005 (textes disponibles sur le site de l'UIT : <http://www.itu.org>) qui commence par ses termes : « Nous, représentants des peuples du monde, ... ». Sur ce texte et sa prétention à constituer une sorte de Constitution de la Société de l'Information : Y. POULLET, « De retour d'un sommet mondial de la Société de l'Information », *RTDI*, 2004, n°18, p. 1 et s.

le patrimoine commun de l'humanité ») et durable de cette société. Le troisième rappelle, à l'heure où l'Internet sans frontières multiplie les heurts entre les conceptions éthiques et philosophiques des peuples, l'absolu respect des droits de l'homme, qu'il s'agisse de la liberté d'expression ou de la vie privée.

Au-delà de ces principes, les textes consacrent une nouvelle approche de la gouvernance de l'Internet. « La gestion internationale de l'Internet devrait s'exercer de façon multilatérale, transparente et démocratique, avec la pleine participation des Etats, du secteur privé, de la société civile et des organisations internationales ». Cette approche dite « *multistakeholders* » fait largement confiance tant à l'autorégulation qu'à la co-régulation des activités liées à l'Internet, y compris dans sa gestion des ressources rares de l'Internet par l'ICANN<sup>64</sup>. Dans le même temps, elle rappelle à la fois la souveraineté des Etats et la nécessité d'une approche cohérente par les organisations internationales publiques multiples et mal coordonnées. L'Agenda de Tunis a mis sur pied un Forum de la Gouvernance de l'Internet qui se réunit annuellement (Athènes (2006), Rio (2007) Hyderabad (2008), Sharm el Shek (2009)), où les représentants des différents *stakeholders* peuvent discuter des questions les plus épineuses concernant le devenir de l'Internet, ainsi, la participation des pays en développement<sup>65</sup>.

## **Titre I. La montée des « régionalismes » : un droit européen de l'Internet ?<sup>66</sup>**

Jean Jacques LAVENUE<sup>67</sup> appelait de ses vœux un « *ius communicationis* » international que préfigure la déclaration de Genève. Dans l'attente, il y a fort à parier qu'entre un Etat Nation incapable à lui seul de réguler un phénomène global et

---

<sup>64</sup> On note la volonté de plus en plus insistante des pays hors Etats-Unis de mettre l'ICANN sous contrôle public international. A cet égard, la récente Communication de la Commission européenne au Parlement européen et au Conseil : « *La gouvernance de l'internet : les prochaines étapes* », Juin 2009.

<sup>65</sup> Sur le succès mitigé de ces Forums, lire J. MALCOM, « Appraising the success of the Internet Governance Forum », disponible sur le site de l'Internet Governance Project : <http://www.internetgovernance.org>

<sup>66</sup> Cette partie du texte renvoie à un article plus fouillé, Y. POULLET « Vers la confiance : vues de Bruxelles : un droit européen de l'Internet ? Quelques considérations sur la spécificité de l'approche européenne », in *Le droit international de l'Internet*, Actes du colloque organisé à Paris, les 18 et 19 novembre 2001, Bruylant, 2002, p. 133 et s.

<sup>67</sup> J.J. LAVENUE, « Cyberspace et droit international : pour un nouveau *ius communicationis* », *Rev. de la recherche juridique-Droit prospectif*, 1996, p. 811-844.

des institutions internationales en mal de légitimité et aux consensus difficiles, des organisations supra-étatiques, régionales fortes d'une certaine cohésion socio-culturelle et donc juridique trouveront dans le phénomène de l'Internet, une justification à l'extension de leurs compétences. Il s'agit de garantir à partir de l'adhésion à des valeurs communes une régulation qui permette le libre établissement des prestataires, la libre circulation des services, bref un marché unique. L'exemple du droit européen de l'Internet atteste de cette montée des « régionalismes ». Il peut servir d'exemple, nous l'espérons, pour la région du Sud est asiatique dans leur volonté de coopération renforcée.

À cet égard, chacun se plaît à souligner la politique européenne énergique d'unification des réglementations en matière de l'Internet politique qui va bien au-delà du principe de subsidiarité<sup>68</sup>. Il s'agit pour les institutions européennes dans une matière aussi évolutive de raccourcir les délais d'adoption et de transposition ; on note l'intervention européenne dans tous les domaines depuis la pédophilie sur Internet jusqu'à certaines dispositions de droit contractuel. Partout, il s'agit d'abord d'harmoniser des contenus réglementaires. Si nous reviendrons sur ces contenus harmonisés, objet du titre II, nous nous attachons ici à deux autres points. Au-delà de l'harmonisation des contenus, on peut souligner les règles nouvelles qui visent à prévenir les conflits ou à lever les barrières au commerce intra-européen (A).

Enfin, on analysera la façon dont la régulation européenne de l'Internet aborde les réglementations en provenance d'autres pays (B).

### **A. Créer un marché interne unique**

Le premier mécanisme est certes l'abolition des barrières tantôt par l'harmonisation des réglementations, tantôt par la création de mécanismes de recours plus aisés en cas de litiges trans-frontières.

Sur le premier point, la directive 98/48/CE du 20 juillet 1998 sur la transparence<sup>69</sup> est remarquable. Considérant que l'harmonisation des règles en

---

<sup>68</sup> Pourtant affirmé récemment par l'article 5 al. 2 et 3 du Traité de la Communauté européenne « domaines qui ne relèvent pas de sa compétence exclusive, la Communauté n'intervient, conformément au principe de subsidiarité, que si et dans la mesure où les objectifs de l'action envisagée ne peuvent pas être réalisés de manière suffisante par les Etats membres et peuvent donc en raison des dimensions ou des effets de l'action envisagée, être mieux réalisés au niveau communautaire ». L'action de la Communauté n'excède pas ce qui est nécessaire pour atteindre les objectifs du présent traité.

<sup>69</sup> Directive mettant en place une procédure pour la fourniture d'informations dans le domaine des standards techniques et des réglementations (J.O., 5 août 1998, L 217). Il s'agit d'une directive amendant pour la troisième

matière de services de la société de l'information décrétée a priori par les instances communautaires est trop risquée voire prématurée, la directive met en place un système d'information, de contrôle et de coordination communautaire de toute initiative nationale en la matière. **Il s'agit là d'éviter la fragmentation du marché interne**, des inconsistances réglementaires ou une frénésie réglementaire qui freinerait le développement de la société de l'information.

Ainsi, la directive impose aux Etats membres de soumettre tout avant-projet de réglementation relatif à un service de la société de l'information, notion définie de manière très large, à une procédure qui permet, le cas échéant, à la Commission de substituer à l'initiative nationale sa propre initiative.

La directive dite « commerce électronique » sur le contenu duquel nous reviendrons (Titre II, Section 1, Sous section 1) va plus loin encore. Son article 3 affirme le principe selon lequel les opérateurs de services de la société de l'information sont soumis à la réglementation et au contrôle de l'Etat sur le territoire duquel ils sont établis<sup>70</sup>. Leur conformité à cette réglementation les autorise à offrir le service dans toute l'Union européenne. C'est ce qu'il est convenu d'appeler la loi du « pays d'origine »<sup>71</sup> qui s'applique tant à l'accès aux services qu'à ces conditions d'utilisation et d'exploitation. Ainsi, si une entreprise d'assurances belge entend permettre l'assurance en ligne à partir de l'ensemble des pays de l'Union Européenne, ne devra-t-elle se soucier que du seul droit belge sans considération des particularités du droit allemand ou du droit des Pays Bas en matière d'accès à la profession ou autres règles relatives aux transactions avec les assurés. La création d'un marché européen des services de l'internet est à ce prix.

Au-delà de ces mécanismes visant à l'harmonisation des règles ou à l'abolition des obstacles réglementaires, divers textes facilitent le règlement des

---

fois la directive 83/89/CE fixant une procédure pour la fourniture d'informations dans le domaine des standards techniques et de la réglementation. À noter qu'au départ, la directive 83/89/CE ne visait que les standards techniques. La directive 98/48 élargit le domaine à l'ensemble des réglementations de la société de l'information.

<sup>70</sup> Certains auteurs ont interprété cet article comme une claire reconnaissance de l'application de la loi du pays d'origine. Ainsi A. CRUQUENAIRE, « La clause de marché intérieur : clef de voûte de la directive sur le commerce électronique », in *Le Commerce électronique européen sur les rails ?*, Cahier du CRID, Bruylant, Bruxelles, 2001, pp. 245-271.

<sup>71</sup> Sur ce principe qui déroge aux règles de droit européen classiques de la libre prestation des services ou de la libre circulation des marchandises, lire Y. de CORDT, C. DELFORGE, T. LEONARD et Y. POULLET, *Syllabus de droit commercial*, Anthémis, Louvain, 2009, pp. 450 à 465 et les références y citées. .

litiges nés des opérations de commerce électronique. Ainsi, plusieurs règlements de l'Union européenne autorisent la saisie de cours et tribunaux d'autres pays de l'Union européenne et reconnaissent aux décisions prises par ces juridictions, une force exécutoire accrue. Certes, l'intervention européenne en la matière ne s'explique pas uniquement par le développement des opérations *on line* mais il faut reconnaître cependant que le développement du commerce électronique et la multiplication des opérations de caractère transnational qui s'en suit, a précipité la réflexion en la matière tant au niveau européen<sup>72</sup> qu'international<sup>73</sup>.

A ce second propos, on ajoutera, au premier mécanisme, la promotion des « procédures extrajudiciaires ou autres procédures comparables : médiation ou conciliation en ligne »<sup>74</sup> qui favorise au-delà des droits parfois divergents, des solutions satisfaisantes. La reconnaissance appuyée de ce type de procédure par l'article 17 de la directive sur le commerce électronique dans le cadre des transactions électroniques du 8 juin 2000 s'élargit à tous les litiges civils et commerciaux dans le cadre de la directive du 21 mai 2008 sur certains aspects de la médiation dans les matières civiles et commerciales..

Enfin, troisième type de mécanisme, les textes réglementaires européens multiplient les obligations de coopération administrative. Ainsi, nombre de textes européens réclament une meilleure coordination des actions menées par les

---

<sup>72</sup> À propos des diverses techniques d'harmonisation, lire M. VAN HUFFEL, « Protection du consommateur et commerce électronique : quelques réflexions au départ du droit de la concurrence », *Ubiquité*, 2001, n° 5, pp. 119 et s.

<sup>73</sup> Cf. à ce propos les travaux de la Convention de la Haye sur la juridiction internationale et les jugements étrangers en matière civile et commerciale qui mentionnent expressément l'importance du commerce électronique (cf. à ce propos le document préliminaire n° 12 « Electronic Commerce and International Jurisdiction », Ottawa, 28 févr.-1<sup>er</sup> mars 2000) (travaux et documents disponibles à l'adresse <http://www.hech.net/workprog/jdgm.html>).

<sup>74</sup> L'Europe soucieuse de promouvoir la confiance des consommateurs et par là même de développer le commerce électronique, souligne la nécessité pour les consommateurs de pouvoir régler leurs litiges de manière efficace et adéquate par la voie de procédures extrajudiciaires ou d'autres procédures comparables également appelées : « Alternative Dispute Resolution Mechanism » selon l'expression anglo-saxonne. En matière d'organes fonctionnant de manière totalement électronique (réception de plaintes, instructions de l'affaire, émission de la sentence) on parle aussi d'O.D.R. (On-line Dispute Resolution Mechanisms). Sur ces mécanismes, P. de LOCHT, « Les Modes de règlement extrajudiciaire des litiges », in *Le Commerce électronique européen sur les rails ?*, M. Antoine et alii, sous la direction d'Etienne Montero, Cahier du CRID, n° 19, Bruxelles, Bruylant, 2001, p. 327 et s. L'article 17 de la directive e-commerce stipule : « Les Etats membres veillent à ce qu'en cas de désaccord entre un prestataire de services de la société de l'information et le destinataire du service, leur législation ne fasse pas obstacle à l'utilisation des mécanismes de règlement extrajudiciaire pour le règlement des différends disponibles dans le droit national y compris par des moyens électroniques appropriés ».

administrations nationales (échanges d'informations, relais de plaintes, ...). Ces administrations nationales jouent en quelque sorte le rôle de guichet unique vis-à-vis de leurs citoyens lorsque ceux-ci ont quelques démêlés avec des opérateurs ou prestataires de services situés dans un autre pays de l'Union européenne. Au-delà, cette coopération entre administrations conduit, on l'espère, à une application plus uniforme, des textes européens.

### **B. Les relations avec les pays tiers : de la politique défensive à une politique plus participative**

Sans doute, et c'est un leitmotiv de leurs discours, les instances européennes sont convaincues de la nécessité de créer un cadre non seulement européen mais mondial du commerce électronique. L'idée de la « Charte Globale » d'Internet prônée par le Commissaire BANGEMANN en septembre 1997 au forum « Interactive Telecom 97 » de l'ITU<sup>75</sup> a été prolongée par de nombreuses discussions, résolutions et débats menés au sein des diverses enceintes européennes<sup>76</sup>.

Si cette coordination « globale » est réclamée et justifie l'action des organes de l'Union au sein des instances internationales publiques comme l'OCDE, l'UIT, le G8 etc., cette volonté ne s'entend pas d'une recommandation de l'Europe à défendre les valeurs auxquelles elle est attachée et de faire ainsi prévaloir une « souveraineté » non plus nationale mais européenne.

Cette défense de la souveraineté européenne s'opère de diverses manières :

- La première attitude est sans doute défensive : c'est celle notamment du juge français dans l'affaire Yahoo déjà analysée<sup>77</sup>, c'est celle du Parlement européen dans

---

<sup>75</sup> Le discours de M. BANGEMANN avait donné lieu à une Communication de la Commission européenne du 4 février 1998 « Globalisation et Société de l'Information : la nécessité d'une coordination internationale renforcée ».

<sup>76</sup> Ainsi, la résolution adoptée le 14 janvier 1999 par le Parlement européen à propos de la communication de la Commission, le débat mené au sein du Conseil des Ministres Telecom, le 30 novembre 1999 : « The I.S of the future responding to the challenges of global electronic commerce ». Cette révolution fait suite aux recommandations émises par le Global Business Dialogue (G.B.D.) sur le futur cadre de la politique réglementaire. Plus récemment, au sein du Parlement européen ou plus exactement de la Commission juridique et du Marché Intérieur, l'avis sur la communication de la Communication au Conseil et au Parlement européen. L'organisation et la gestion de l'Internet – Enjeux internationaux et européen (COM (2000) 202. C5-0263/20002000/2140 (COS).

<sup>77</sup> Analysée supra, Titre I, Sous titre I, Sous Titre II, Section I.

l'affaire Echelon<sup>78</sup> ou plus récemment à propos du contrôle des passagers de transport aérien<sup>79</sup>. Il s'agit d'interdire certaines pratiques extraterritoriales ou du moins d'en limiter les effets vis-à-vis des citoyens européens, et ce, au nom de valeurs sociales jugées primordiales par un Etat donné ;

- La deuxième attitude possible est plus ouverte : il s'agit, sans renier les valeurs européennes, de chercher, sans impérialisme outrancier, dans le respect des systèmes des pays tiers, la protection adéquate des libertés et valeurs prônées par l'Europe. L'article 25 de la directive européenne 95/46 en matière de protection des données personnelles<sup>80</sup> et plus encore l'application récente qui en a été faite dans le cadre des négociations entre l'Union européenne et les Etats Unis illustrent cette deuxième voie<sup>81</sup>. A travers ce texte, il s'agit de reconnaître que les deux entités US et EU partagent les mêmes valeurs de défense de protection des données même si les garanties peuvent être trouvées selon des modalités différentes dont on attend une effectivité similaire : ainsi, est prônée l'adéquation de l'autorégulation ou, plutôt, l'autorégulation américaine spécifique aux flux Europe- Etats-Unis et volontairement acceptée par les entreprises américaines aux exigences de l'approche législative européenne pour légitimer certains transferts internationaux vers ce dernier pays.

---

<sup>78</sup> Cf. le rapport présenté par G. SCHMIDT sur l'existence d'un système global de surveillance pour l'interception de communications privées et commerciales (Système d'interception Echelon) au comité temporaire sur le système d'interception Echelon, 18 mai 2001 (PE 305.391) et la Résolution n° 15 proposée par le rapport SCHMIDT cité note précédente : « Urges the Commission and member States to develop appropriate measures to promote, develop and manufacture European Encryption Technology and software and above all to supports projects aimed at developing user friendly open-source encryption software ».

<sup>79</sup> C'est l'affaire des « Passenger Name Record » déjà évoquée supra, note 37 et la référence y reprise. Pour l'ensemble de l'affaire et ses multiples rebondissements, lire Pour une analyse plus complète de la proposition au regard des principes de protection des données, lire O. DE SCHUTTER, T. OJANEN, M. SCHEININ, « Thematic legal study: opinion on the draft proposal for a Council framework decision on the use of PNR data for law enforcement purposes », *Fundamental Rights Agency*, 6/10/2008 et F. DUMORTIER et Y. POULLET, **La protection des données à caractère personnel dans le contexte de la construction en piliers de l'Union européenne, in *Revue Lamy Droit de l'immatériel*, issue 29, pp. 76-86**

<sup>80</sup> Sur la protection « adéquate » ou comment un ordre étatique peut imposer simplement des valeurs aux pays tiers dans la société globale de l'information, voir Y. POULLET et B. HAVELANGE, « *Preparation of a methodology for evaluating the adequacy of the level of protection of individuals with regard to the processing of personal data* », Office of Publication of the European Communities, 1998, Annex to the Annual Report 1998 (XVD/5047/98) of the WG art. 29 of Dir. 95/46/CE et sur ces critères du caractère adéquat, les documents publiés et approuvés par le Groupe de protection des personnes à l'égard du traitement de données à caractère personnel, groupe dit « de l'art. 29 », ainsi le WP 12 (5025/98) « Applying articles 25 et 26 » (juillet 98).

<sup>81</sup> Décision de la Commission 2000/520/CE de la Commission conformément à la directive 95/46/CE relative à la pertinence de la protection assurée par les principes de la « sphère de sécurité » et par les questions souvent posées y afférentes, publiés par le Ministère du Commerce des Etats-Unis d'Amérique, J.O.C.E., 25 août 2000, L. 215, p. 7 et s.

- Enfin, une troisième voie est celle de l'entrée des instances européennes dans les organes d'autoréglementation. Cette troisième voie est celle suivie par les instances européennes à propos de « l'organisation et la gestion de l'Internet » en clair, l'entrée de la Commission européenne comme telle dans l'ICANN qui gère l'attribution des noms de domaine au niveau mondial. On a déjà noté la déclaration récente de la Commission européenne sur la Gouvernance de l'Internet qui entend affirmer le rôle politique de la puissance publique dans la conduite et la gestion du développement de l'Internet.

## **TITRE II Le contenu de la régulation européenne de l'Internet quelques traits marquants**

Par régulation européenne, on entend tant celle du Conseil de l'Europe dont on sait qu'il réunit outre les pays de l'union européenne, nombre de pays de l'ancienne Union Soviétique, soit 47 états membres. Le Conseil a certes un domaine de compétence bien plus restreint que celui de l'Union européenne compétente depuis le traité d'Amsterdam dans tous les domaines depuis les questions économiques et sociales jusqu'aux questions de droits de l'homme, de sécurité intérieure, de politique étrangère et de coopération judiciaire. Le Conseil défend les droits de l'homme et garantit l'application effective de la Convention européenne des droits de l'homme et recherche des solutions aux problèmes de société (xénophobie, discrimination envers les minorités, crime organisé,...). Le Conseil, au-delà de la Convention des droits de l'homme a multiplié les conventions et recommandations dans des domaines touchant à certains thèmes particulièrement important dans la régulation de l'internet, ainsi en matière de protection de la vie privée, de la liberté d'expression et de criminalité informatique. Nous reviendrons sur ces textes majeurs. Précisons cependant une caractéristique majeure de ces Conventions du Conseil. Elles sont ouvertes à la signature des pays tiers et peuvent ainsi constituer la base d'une régulation internationale de l'Internet. Ainsi, la Convention sur la cybercriminalité de 2001 a été ratifiée en 2006 par le Congrès américain et nombre de pays de tous les continents l'ont signée.

Quatre domaines de régulation sont étudiés :

- Celui des transactions électroniques : il s'agit essentiellement de définir un cadre dans lequel les opérations de commerce électronique pourront se développer en toute confiance ;
- Celui des libertés qu'il s'agisse de celles assurées par la protection des données de la liberté d'expression;
- Celui de la criminalité informatique qui contient à la fois des règles de droit pénal matériel et de droit pénal procédural y compris de coopération ;
- Celui des droits de propriété intellectuelle où la politique européenne oscille entre affirmations et doutes.

Un maître-mot justifie l'action européenne : la confiance<sup>82</sup>. Il s'agit en effet de conjurer les craintes des internautes et des opérateurs du réseau, en rassurant tantôt l'un, tantôt l'autre tantôt l'un et l'autre que les opérations du commerce électronique respecteront les libertés essentielles des individus tout en offrant la sécurité des transactions et des investissements. Le législateur français l'a bien compris, lui qui adoptait récemment une loi globale sur ces différents aspects et l'a intitulée « Loi pour la confiance dans l'économie numérique »<sup>83</sup>. Pour contribuer à une telle confiance, la liste des infractions pénales a été adaptée à la réalité nouvelle en même temps que les moyens d'investigation tiennent désormais compte des caractéristiques des systèmes d'information.

## **Sous-Titre I: Les opérations : un cadre juridique pour les transactions juridiques**

### **Section I – Les directives de base**

Trois directives mettent en place les principes fondamentaux et généraux propres aux acteurs et opérations du commerce international : la directive relative à certains aspects juridiques du commerce électronique du 8 juin 2000<sup>84</sup> et celle sur la protection juridique des signatures électroniques du 13 décembre 1999<sup>85</sup>. Ces directives proposent une traduction très originale et souvent moins souples des lois modèles que nous avons évoquées plus haut.

Sans prétendre être exhaustif, relevons quelques uns de leurs principes. On notera à propos des acteurs que l'accès au marché des opérateurs de services de la société de l'information<sup>86</sup> ne peut être soumis à des conditions supplémentaires à celles déjà existantes pour l'offre non électronique des mêmes services. Notons

---

<sup>82</sup> A cet égard, nos conclusions in « le droit européen de l'internet », *op. cit.*, p. 172.

<sup>83</sup> En abrégé : la LCEN. Loi n° 2004-575, 21 juin 2004 pour la confiance dans l'économie numérique, J.O. 22 juin 2004, p.11168. Sur cette loi, les commentaires repris dans le numéro spécial du J. Cl. Ed Communication Commerce électronique, Sept. 2004.

<sup>84</sup> Directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information et notamment du commerce électronique, dans le marché intérieur (directive dite « commerce électronique »), publiée in J.O., 17 juillet 2000, L 178, pp. 1-16.

<sup>85</sup> Directive 1999/93/CE du Parlement européen et du Conseil du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques (directive dite « signature électronique »), publiée in J.O., 19 janv. 2000, L 13, pp. 12-20.

<sup>86</sup> On notera que la traditionnelle distinction entre « commerçants » et « professions libérales » et « non commerçants » est, en ce qui concerne les principes fondamentaux, abolie.

toutefois que les opérateurs de services de certification de signature électronique pourront être soumis à des conditions d'interopérabilité et au contrôle du respect de certaines conditions s'ils entendent que les signatures à l'appui desquelles ils émettent des certificats puissent être dotées d'une valeur probante particulière. Ce principe du libre accès est seulement tempéré par des obligations accrues de transparence, juste contrepartie de l'absence de « face à face » de l'offreur et du demandeur sur Internet. Ainsi, on priera le prestataire des services de la société de l'information de décliner son identité, sa localisation, le moyen de l'atteindre et on l'astreindra à rendre accessible directement et par des moyens aisés les conditions, codes de conduite et autres auxquelles il accepte de se soumettre.

A propos des opérations du commerce électronique, un premier principe est l'obligation faite aux Etats membres de ne point discriminer directement ou indirectement les opérations du commerce électronique par des prescrits légaux affectant la valeur, l'efficacité ou la force contraignante de l'utilisation de l'électronique, et ce, à quelque stade de l'opération<sup>87</sup>.

Ce principe de non discrimination vaut également pour la signature électronique et on ajoute même que l'équivalence de valeur juridique de la signature électronique à celle de la signature manuscrite peut même être obtenue sous certaines conditions qui tiennent tant à la qualité des services du prestataire qu'à la robustesse et à la nature de la signature électronique. Au principe de non discrimination, s'ajoute ainsi celui d'équivalence fonctionnelle<sup>88</sup>, principe qui affirme la nécessité pour le droit de reconnaître un statut égal aux opérations menées électroniquement lorsqu'il est démontré qu'elles remplissent les mêmes fonctionnalités que celles accomplies avec les moyens traditionnels. Ainsi, si la signature électronique permet d'accomplir les fonctions d'identification et d'authentification que la signature manuscrite, ainsi si l'ordinateur permet grâce à des logiciels appropriés de donner à

---

<sup>87</sup> Sur le principe de « non discrimination », comme principe général par lequel le droit accueille les développements technologiques, lire nos réflexions in *La technologie et le droit : du défi à l'alliance*, in Liber Amicorum G. HORSMANS, Bruylant, 2004, p. 956 et s.

<sup>88</sup> Selon le Guide pour l'incorporation de la loi type dans le droit interne, cette approche repose « sur une analyse des objectifs et des fonctions de l'exigence traditionnelle de documents papier et vise à déterminer comment ces objectifs ou fonctions pourraient être assurés au moyen des techniques du commerce électronique ». Les messages informatisés qui rempliraient les mêmes fonctions que les documents papier pourraient ainsi bénéficier du même degré de reconnaissance juridique<sup>3</sup>. Cette analyse va de pair avec le principe de neutralité technologique, généralement compris comme la nécessité d'une égalité de traitement des activités en ligne et hors ligne et d'une impartialité vis-à-vis des techniques<sup>4</sup> utilisées pour communiquer, transmettre ou stocker de l'information.

l'archive électronique, les mêmes garanties que la copie papier, ainsi, si les formalités parfois réclamées par le droit peuvent voir leur fonction protectrice ou de solennités réalisée adéquatement par voie électronique<sup>89</sup> et on peut multiplier les exemples d'application de ce principe<sup>90</sup>.

Ce principe est tempéré par l'exigence de considérer la transaction électronique comme le résultat d'une procédure à diverses étapes afin d'assurer que le consentement auquel elle aboutit soit éclairé, complet et certain. Cette découpe apparaît comme un juste contrepoids aux risques que fait courir l'utilisation d'une technologie de l'instantané entre contractants « à distance »<sup>91</sup>.

Une troisième directive mérite un rapide commentaire. Il s'agit de la directive du 11 septembre 2007<sup>92</sup> amendant la directive sans frontières pour l'adapter à la réalité de la télévision numérique et interactive accessible désormais via internet y compris à partir de son mobile. La directive est applicable aux services audiovisuels à la demande et aux services accessibles au moment souhaité (webcasting, live streaming, etc.). La directive analyse les fournisseurs de tels services comme des éditeurs, affirme le principe du pays d'origine, élargit comme la directive « commerce électronique », les obligations d'information et fixe des règles en matière de service universel et de sponsoring.

## **Section II : En ce qui concerne quelques aspects ou opérations spécifiques**

L'Union européenne complète le cadre proposé par les deux directives analysées ci-dessus par des dispositions, d'une part, relatives à la protection des consommateurs et, d'autre part, concernant la soi-disante « monnaie » électronique.

A propos des premiers, la conviction européenne selon laquelle le développement de la société de l'information implique obligatoirement la confiance

---

<sup>89</sup> M. DEMOULIN et E. MONTERO, « La conclusion des contrats par voie électronique », in *Le processus de formation du contrat. Contributions comparatives et interdisciplinaires à l'harmonisation du droit européen*, sous la direction de M. FONTAINE, Bruxelles, Bruylant et Paris, L.G.D.J., 2002, p. 693 à 788 ; des mêmes auteurs, « Le formalisme contractuel à l'heure du commerce électronique », in *La théorie générale des obligations, suite*, Formation permanente – CUP, octobre 2002, vol. 57, pp. 99-181.

<sup>90</sup> H. JACQUEMIN, *Le formalisme de protection de la partie faible au rapport contractuel*, Thèse défendue à Namur, 2009, à paraître chez Larcier, Bruxelles.

<sup>91</sup> A ce propos, on citera la célèbre formule de E. KATSCH ( *Law in a Digital World*, op.cit., p. 129 ) : « Paper contracts bind parties to an Act, Te electronic contract binds parties to a process »

<sup>92</sup> Directive 2007/55/ UE.

des consommateurs<sup>93</sup> a justifié tant des affirmations de principes, telles la Résolution du Conseil de l'Europe du 19 janvier 1999 à propos de la dimension « consommateurs » de la Société de l'information, véritable Charte des droits du consommateur - internaute<sup>94</sup> que l'adoption de textes ayant une valeur normative plus directe. On note, à cet égard, la directive sur les contrats à distance du 20 mai 1997<sup>95</sup> qui étend au monde du commerce électronique, une série de droits impératifs affirmés pour toute transaction conclue à distance et oblige l'offreur de services à émettre sur « support durable » la trace des transactions opérées par voie électronique<sup>96</sup>. On signale enfin la directive relative à l'offre à distance des services financiers (y compris services d'assurance) visant des consommateurs<sup>97</sup>. Cette directive élargit notablement les obligations de transparence et d'informations, les délais de réflexion et de renonciation et prévoit des mécanismes efficaces et adéquats de plaintes et de solution des litiges. Parmi ces services, on trouve la mise à disposition de services de paiement à distance. Ce qui introduit le second sujet.

Ce second sujet a fait l'objet d'une intervention normative importante des instances européennes : la monnaie électronique<sup>98</sup> est un élément indispensable pour

---

<sup>93</sup> Cette conviction est rappelée avec force par les commentaires de la Commission européenne dans sa réponse en date du 21 avril 1999 à la demande de la FTC américaine de réactions académiques et de commentaires publiés suite au rapport de la FTC : « US Perspectives on Consumer Protection in the Global Electronic Marketplace. US Federal Trade Commission Notice requesting academic papers and public comments ».

<sup>94</sup> La Résolution du Conseil des Ministres en charge de la consommation du 19 janvier 1999 reprend un certain nombre de principes ainsi notamment :

- celui de la transparence et du droit de recevoir une information suffisante et fiable avant et après transaction ;
- celui de la non discrimination dans l'accès aux produits et services et de l'attention aux consommateurs vulnérables ;
- celui de la distribution équitable des risques et des responsabilités ;
- celui de la participation des organisations de consommateurs dans la protection des intérêts des consommateurs ;
- celui de l'information et de l'éducation des consommateurs, aptes à les rendre capables de développer des savoir faire appropriés ; .....

<sup>95</sup> Directive 97/7/CE, JO, 4 juin 1997, L 144/19.

<sup>96</sup> Sur cette notion, lire M. DEMOULIN, « La notion de « support durable » dans les contrats à distance : une contrefaçon de l'écrit ? », *Rev. Eur. Droit de la Consommation*, 2000, p. 361 et s. 86

<sup>97</sup> Sans doute, faudrait-il mentionner également, même si l'objet est plus large que les opérations du commerce électronique, la proposition de directive sur les pratiques commerciales déloyales du 17 juin 2003 (COM (2003) 0356) qui sera incessamment approuvée.

<sup>98</sup> Notion définie largement par la directive du Parlement et du Conseil (2000/28/CE) du 18 septembre 2000 modifiant la directive 77/780/CE sur la coordination des lois, règlements et dispositions administratives relatives au démarrage et à la poursuite des activités des institutions de crédit.

assurer le développement du commerce électronique<sup>99</sup>.

La communication et la recommandation de la Commission européenne de juillet 1997<sup>100</sup> instituent en particulier, outre des devoirs d'information sur l'utilisation du moyen de paiement et ses conséquences, des règles claires de répartition de responsabilités entre émetteur et utilisateur du moyen de paiement, en cas de vol, de fraude, perte ou erreur et des mécanismes efficaces de règlement des litiges. Des directives sont adoptées ou en chantier. Deux directives du 18 septembre 2000 visent, d'une part, à harmoniser les réglementations nationales relatives aux institutions de crédit en élargissant le nombre d'institutions aptes à émettre de la monnaie électronique<sup>101</sup> et, d'autre part, à contrôler les opérations de ces institutions. Il s'agit de s'assurer de la stabilité et de la robustesse des émetteurs de moyens de paiement tout en distinguant différents statuts suivant l'importance des risques liés au type de moyens de paiement émis<sup>102</sup>. La directive du 25 octobre 2007<sup>103</sup> sur les services de paiement dans le marché intérieur se veut une solution globale à l'ensemble des questions posées par l'émission de monnaie électronique et aux services qui l'entourent. Elle couvre les opérations de paiement à partir de mobiles ou autres supports électroniques, elle élargit le champ d'application à tout émetteur de cartes prépayées qui peuvent servir de paiement auprès de tiers et soumet leurs activités à autorisation ainsi qu'à des obligations de capital minimum et autres garanties. Surtout la directive impose des devoirs d'information stricts sur le service rendu, l'émetteur, les possibilités de révocation et le partage des risques entre l'émetteur, l'utilisateur et le tiers, bénéficiaire du paiement. Enfin, on ajoute le principe de non discrimination des utilisateurs et le droit de ces derniers à des recours auprès d'instances privées.

---

<sup>99</sup> Cf. Communication de la Commission sur le commerce électronique du 16 avril 1997 (COM (97)157), «Une initiative européenne en matière de commerce électronique ». La Commission notait que le commerce électronique ne se développerait pas « sans des moyens de paiement électronique robustes, conviviaux, efficaces et sûrs ».

<sup>100</sup> Recommandation relative aux transactions par des instruments de paiement électronique et en particulier les relations entre émetteur et porteur, COM (97)353 (une étude sur l'application de cette recommandation a été publiée le 20 mars 2000).

<sup>101</sup> Cf. également la Communication de la Commission sur « Un nouveau cadre juridique pour les paiements dans le marché interne, COM (2003) 718 ».

<sup>102</sup> A noter à propos des moyens de paiement par mobilophonie, le « EU Blueprint on Mobile payment », document de travail du 12 juin 2003 et la communication de la Commission du 30 juin 2004 (COM (2004) 447).

<sup>103</sup> Directive 2007/56, JOUE

On ajoutera des décisions européennes à propos de la lutte contre le blanchiment d'argent et la contrefaçon des moyens de paiement non liquides<sup>104</sup>.

---

<sup>104</sup> Ainsi la décision cadre 2001/413/HA du 28 mai 2001 sur la fraude et la contrefaçon des moyens de paiement non liquides et les communications et plan d'action du 9 février 2001 sur la prévention des fraudes et contrefaçons des moyens de paiement non liquides (COM (2001)11).

## **Sous-Titre II : Les valeurs : un difficile équilibre entre « libertés » et « sécurité » du réseau.**

Le Conseil de l'Europe, l'Union européenne comme les Etats Unis reconnaissent la liberté d'expression comme une valeur fondamentale du réseau de l'Internet, même si l'une et l'autre de ces régions du monde se voient confrontées à la nécessité de fixer certaines limites à cette liberté lorsque l'exercice abusif de celle-ci nuit à autrui par des contenus illégaux ou dommageables. Sans doute, certaines nuances entre les réponses de l'une et de l'autre méritent d'être soulignées.

Plus grave est le fossé qui sépare ces deux régions en ce qui concerne la protection de données à caractère personnel. L'héritage de la convention n° 108 du Conseil de l'Europe<sup>105</sup> a conduit l'Union européenne à adopter en 1995 une directive de base<sup>106</sup> en la matière et plus récemment, une seconde directive dite « sectorielle »<sup>107</sup> a adapté les principes de la première aux risques plus spécifiques des réseaux de communication électronique. Outre Atlantique, hormis certaines législations très spécifiques, confiance est faite au marché et à son autorégulation<sup>108</sup> pour assurer la protection des données à caractère personnel.

Les attentats du 11 septembre ont modifié quelque peu l'attitude européenne en matière de protection des données. L'obsession de la lutte contre le terrorisme a conduit au-delà des dispositions sur la cybercriminalité<sup>109</sup> à l'adoption de quelques mesures de procédure pénale dont l'ampleur selon de nombreux auteurs risque de mettre en cause les libertés individuelles. Nous y reviendrons.

---

<sup>105</sup> Convention pour la protection des personnes à l'égard du traitement des données à caractère personnel faite à Strasbourg. Cf. les nombreuses recommandations émises depuis sur base de cette convention reprises sur le site du Conseil de l'Europe : <http://www.coe.int>

<sup>106</sup> Directive 95/46/CE relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation des ces données, J.O., n° L. 281 du 23 novembre 1995, p. 31. Sur cette directive, lire entre autres, M. H. BOULANGER, C. de TERWANGNE, T. LEONARD, S. LOUVEAUX, D.MOREAU, Y. POULLET, « La protection des données à caractère personnel en droit communautaire, *JTDE*, 1997, p. 121-127 ; p. 145- 155 ; pp.173-179.

<sup>107</sup> Directive 2002/58/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques, JOCE, 31 juillet 2002, L.201, p. 37 à 47. Sur cette directive, J. DHONT et K.ROSIER, « Directive Vie privée et communications électroniques », *Ubiquité*, 2003/15, p. 7 et s.

<sup>108</sup> Sur l'approche américaine comparée à celle européenne, lire P.A. SCHWARTZ et J. REIDENBERG, *Data Privacy Law*, Michie, New York, 1996

<sup>109</sup> Convention du Conseil de l'Europe sur la cybercriminalité, Budapest, 23 novembre 2001.

## **Section I . Le délicat équilibre entre la liberté d'expression et d'autres intérêts dignes de protection**

Le Conseil de l'Europe affirme d'emblée la nécessité de non discrimination entre les auteurs de propos qu'ils s'expriment sur l'Internet ou au contraire par les modes traditionnels<sup>110</sup> et répète à l'envie que la liberté s'entend y compris de propos choquants voire dérangeants<sup>111</sup>. Les attendus suivants de la recommandation du 26 septembre 2007<sup>112</sup> résume bien les divers axes de la politique du Conseil en la matière : *« Ayant à l'esprit l'impact potentiel, tant positif que négatif, que les technologies et services de l'information et de la communication peuvent avoir sur la jouissance des droits de l'homme et des libertés fondamentales dans la société de l'information, ainsi que le rôle et la responsabilité spécifiques des Etats membres pour la protection et la promotion de ces droits ; Soulignant, à cet égard, que le développement des technologies et des services de l'information et de la communication devrait contribuer à ce que toute personne jouisse des droits garantis par l'article 10 de la CEDH, dans l'intérêt de chacun et dans celui de la culture démocratique de toute société ; Rappelant la Recommandation no R (99) 14 du Comité des Ministres sur le service universel communautaire relatif aux nouveaux services de communication et d'information, qui souligne la nécessité de développer constamment ces services pour promouvoir le droit de toute personne à exprimer, rechercher, recevoir et transmettre des informations et des idées, au bénéfice de chaque individu et de l'ensemble de la société ; Soulignant l'importance d'un accès gratuit ou à des conditions abordables aux contenus et aux services au vu de la convergence des secteurs des médias et des nouveaux services de communication, et de l'apparition de plates-formes et de services communs entre les opérateurs de télécommunication, les fabricants de matériel et de logiciels, les organes de la presse*

---

<sup>110</sup> [Déclaration](#) sur la liberté de la communication sur l'Internet, adoptée le 28 mai 2003. Cette déclaration est suivie par nombre de recommandations, en particulier celle du 7 novembre 2007 réaffirmant la nature de service public de l'Internet et donc le droit d'accès de chacun au réseau à un prix abordable e celle du 26 septembre 2007 relative à la promotion de la liberté d'expression et d'information dans le nouvel environnement de l'information et de la communication.

<sup>111</sup> CEDH *Handyside c. R.U.*, 7 décembre 1976, §49. A propos de cette décision et de son actualité dans la société de l'information, P.F. DOCQUIR ; « Le droit de réponse 2.0 ou la tentation d'un droit subjectif d'accès à la tribune médiatique », in *Les propos qui heurtent, choquent ou inquiètent*, Rev de la faculté de droit de l'ULB, Bruylant, Bruxelles, 2006, pp. 289 et s.

<sup>112</sup> Citée note 106

*écrite, du secteur de la radiodiffusion et des nouveaux services de communication, les fournisseurs d'accès à Internet et les autres opérateurs de réseaux de la prochaine génération ; Rappelant la Déclaration de 2005 du Comité des Ministres sur les droits de l'homme et l'Etat de droit dans la société de l'information, qui reconnaît que l'accès limité ou l'absence d'accès aux technologies de l'information et de la communication (TIC) peut priver les individus de la capacité d'exercer pleinement leurs droits de l'homme et leurs libertés fondamentales.»*

En ce qui concerne cette fois, l'Union européenne, l'affirmation de la liberté d'expression est plus indirecte. Les articles 12 et suivants de la directive « commerce électronique » déjà citée reconnaissent ainsi implicitement le principe de la liberté d'expression sur l'Internet, en exonérant, sur le modèle du DMCA américain<sup>113</sup>, les opérateurs de réseaux, les fournisseurs d'accès et les hébergeurs de toute responsabilité pour les contenus illégaux ou dommageables qu'ils véhiculent ou hébergent sans le savoir<sup>114</sup> et en les exonérant de toute obligation de surveillance des contenus hébergés. La solution de la Directive ne dit cependant rien sur la responsabilité des moteurs de recherche ou des plate-formes du Web 2.0 comme YouTube ou Facebook, ce qui n'est pas sans causer des jurisprudences contradictoires en la matière, les juges appliquant à ces nouveaux intermédiaires tantôt une responsabilité d'éditeurs, tantôt par une analyse plus serrée de la fonction mise en cause par l'événement dommageable, une responsabilité tantôt de courtiers, d'éditeurs de service ou de simples hébergeurs<sup>115</sup>.

La nécessité de lutter tant contre la pornographie infantile<sup>116</sup> que contre le racisme et la xénophobie<sup>117</sup> amène cependant progressivement l'Union européenne à adopter de nombreux textes à travers lesquels elle opère une « balance » entre la

---

<sup>113</sup> Sans doute, faudrait-il être plus nuancé. A propos de l'origine américaine de la disposition européenne et de la comparaison entre les deux textes, lire R. JULIA BARCELO et KOELMAN, K.J. « Intermediary Liability in the e-commerce directive : so far so good but it's not enough », *CLSR*, 16, n° 4, 2000, 213-239.

<sup>114</sup> L'article 15 de la directive « Commerce électronique » en outre les soustrait à tout devoir de surveillance ou de contrôle préventif.

<sup>115</sup> A cet égard, E. MONTERO, « Les responsabilités liées au Web 2.0 », *RDTI*, 2009, pp. 363 et s.

<sup>116</sup> Cf. notamment la Décision 2004/68/JHA (J.O., L 13/44, 20.1.2004) du Conseil du 22 décembre 2003 sur l'exploitation sexuelle des enfants et la pornographie infantine.

<sup>117</sup> Ainsi la recommandation du 24 septembre 1998 déjà citée reprend en annexe « des lignes directrices pour le développement des systèmes nationaux d'autorégulation ».

liberté d'expression et ces autres intérêts.

A cet égard, on note que si les premiers textes européens, adoptés dans la foulée des décisions américaines suite à la déclaration d'inconstitutionnalité du Decency Act<sup>118</sup>, se référaient exclusivement à l'autorégulation et aux développements technologiques pour assurer le développement d'un « réseau sûr », progressivement<sup>119</sup>, l'intervention de l'Etat se fait plus pressante, tout d'abord, par un encadrement de l'autorégulation, ensuite, en instituant une coopération maximale entre opérateurs d'Internet et autorités publiques dans la mesure où les textes imposent aux premiers l'obligation de garde préventivement, trace des utilisations de chacun<sup>120</sup> et, enfin, par l'obligation mise à charge des intermédiaires de mettre sur pied leurs propres systèmes de contrôle en ce qui concerne en tout cas la pornographie infantile<sup>121</sup>. Une décision-cadre du 28 novembre 2008<sup>122</sup> combat le racisme et la xénophobie sur l'Internet.

## **Section II. La protection des données à caractère personnel**

L'histoire de la protection des données prend naissance avec l'article 8 de la Convention européenne des droits de l'homme de 1950. La disposition rejointe par d'autres, telles l'article 12 de la Déclaration des Droits de l'Homme ou l'article 17 du Pacte international relatif aux droits civils et politiques laisse concevoir la vie privée comme le « droit d'être laissé seul »<sup>123</sup>, lié au droit à l'intimité des personnes. Celui de ne pas voir révéler des informations liées à sa « sphère privée », qu'elle soit

---

<sup>118</sup> Sur l'historique du Decency Act et sa condamnation par la Cour constitutionnelle américaine, lire G. GRANGER, Liberté d'expression et réglementation de l'information dans le cyberspace, in *Les dimensions internationales du droit du cyberspace*, op. cit., p. 90 et s.

<sup>119</sup> Pour une liste des nombreuses recommandations, décisions et communications prises auparavant en la matière, lire M. D'Udekem-Gevers et Y. POULLET, Concerns from a European User Empowerment Perspective in Internet Content Regulation, *Communications et Strategies*, Montpellier, 2001.

<sup>120</sup> Cf. à ce propos la décision du Conseil du 29 mai 2000 pour combattre la pornographie infantile sur Internet, ce qui, notons-le, est en contradiction avec l'article 15 de la directive sur certains aspects du commerce électronique qui exonère les intermédiaires de l'obligation de mettre en place des mesures de surveillance.

<sup>121</sup> Cf. à ce propos la décision du Conseil du 29 mai 2000 pour combattre la pornographie infantile sur Internet, ce qui, notons-le, est en contradiction avec l'article 15 de la directive sur certains aspects du commerce électronique qui exonère les intermédiaires de l'obligation de mettre en place des mesures de surveillance.

<sup>122</sup> Décision-cadre 2008/213 JAI du 28 novembre 2008 combattant le racisme et la xénophobie

<sup>123</sup> Le fameux « Right to be left alone » défendu par S. WARREN et L. BRANDEIS dans leur article fameux : « *The right to privacy* », 4, *Harvard Law Rev.*, 193 (1890).

physique : le domicile familial ou qu'elle soit l'expression d'une relation à autrui, le secret de la correspondance<sup>124</sup>.

Sans doute, les premières législations de protection des données étaient-elles de ce fait focalisées sur les risques d'atteinte à l'intimité des personnes et sur les dangers d'une surveillance des individus<sup>125</sup>. La référence exclusive à la vie privée et l'importance des données sensibles dans les premières législations traduisent leur filiation avec l'article 8 de la Convention européenne. Cette première conception explique également que la première législation, celle du Land de Hesse en 1970 se soit concentrée sur les seuls traitements d'information opérés par l'Etat.

Progressivement, il est cependant constaté que les technologies de l'information et de la communication accentuent le déséquilibre d'informations entre les personnes concernées et les responsables des traitements qu'ils soient publics ou privés. Ces technologies menacent dès lors non seulement l'intimité ( la vie privée-intimité ) mais l'ensemble des libertés individuelles ( la vie privée-libertés ) ainsi, la liberté d'obtenir un crédit, un logement, celle de se déplacer, etc.<sup>126</sup>, mais également des libertés consacrées par d'autres articles de la Convention européenne des droits de l' Homme, ainsi la liberté d'expression<sup>127</sup>, celle de saisir la justice<sup>128</sup>, la liberté de vote, etc En même temps, elles

---

<sup>124</sup> A ce propos, la Recommandation 428 (1970) du Comité d'experts du Conseil de l'Europe portant déclaration sur les moyens de communication de masse et les droits de l'homme, Annales de la Conv. Vol. 13, 1970, p. 65.

<sup>125</sup> La loi du Land de Hesse est sans doute un bel exemple de cette approche, de même que la loi française de 1978, prise en réaction au projet SAFARI. Sur cette focalisation des premières législations sur la vie-privée intimité et la nécessité d'élargir le débat, lire entre autres, D.J. SOLOVE, "Conceptualizing Privacy", 90 *California Law Review*, 2002, 1085 et s; P.BLOK, *Het recht op privacy*, Boom Juridische uitgevers, 2003

<sup>126</sup> La protection des données constitue le moyen d'assurer la vie privée et sa consécration est une conséquence directe de l'obligation positive des Etats d'assurer le respect de la vie privée au sens le plus large

<sup>127</sup> Qui ne voit que la protection des données est le meilleur garant de la liberté d'expression dans la mesure où le contrôle de l'expression de chacun permis par les technologies modernes de l'information et de la communication peuvent amener les citoyens voire les journalistes à limiter leur expression par peur des conséquences.

<sup>128</sup> On sait la lutte que nombre d'autorités de contrôle en matière de protection des données ont mené contre l'utilisation par des entreprises de renseignements relatives à l'introduction de recours judiciaires qui leur permettaient de cibler des consommateurs « agressifs » ou des employés « revanchards » De même, l'informatisation du judiciaire et de la diffusion des décisions judiciaires font craindre la mise en péril des droits de la défense ( A ce sujet D. MOREAU-Y. POULLET, « *La justice au risque de la vie privée* », in Phénix et la procédure électronique, Travaux de la CUP, 02-2006, Vol. 85, p. 87 à 141.

engendrent un risque important de discrimination en cas d'utilisation de données inexactes ou surtout disproportionnées<sup>129</sup>.

C'est le mérite de la Convention n° 108, d'élargir le débat dans deux directions : le premier est d'instituer en vue de la protection des données à caractère personnel certaines restrictions à l'utilisation de celles-ci, de créer des obligations de sécurité et administratives à charge de ceux qui traitent des données à caractère personnel et de restreindre, d'une part, la liberté des responsables de traitements, entreprises ou associations, en particulier leur liberté d'entreprendre ou d'associations et, d'autre part, les prérogatives d'intérêt général de l'Etat. Ainsi sont affirmés des principes nouveaux de nature à prévenir les risques spécifiques nés de l'utilisation des technologies de l'information et de la communication (collecte à l'insu des personnes, détournement de finalité etc...) : principes de la collecte loyale, de la finalité légitime et de la proportionnalité du contenu des traitements, principe de l'information des personnes concernées et de leur droit d'accès, principe de sécurité, et liste de données sensibles. .. Un protocole additionnel de 2001 devait ajouter deux principes majeurs : la nécessité d'une autorité indépendante et le principe du transfert de données vers les seuls pays tiers offrant une protection adéquate.

La directive cette fois de l'Union européenne, directive 95/46, permet d'assurer par l'harmonisation poussée des règles en matière de protection des données une libre circulation des données dans l'Union européenne tout en maintenant une certaine marge de manœuvre pour des Etats membres. Elle fixe les conditions de traitement des données à caractère personnel en distinguant du régime général, celui des données sensibles. Elle crée des obligations de déclaration et de sécurité pour les responsables de traitement, confère à la personne concernée des droits visant à permettre le contrôle par celle-ci de son image informationnelle et de sa circulation. Enfin, elle reconnaît les compétences des autorités nationales, indépendantes de contrôle et crée deux groupes de travail européens, chargés tant d'une veille technologique que de coordonner les points de vue<sup>130</sup>.

La seconde directive « sectorielle » applique les principes de la directive de

---

<sup>129</sup> A ce propos, le principe repris dans toutes les législations de protection des données suivant lequel les données doivent être pertinentes, adéquates et non excessives par rapport aux finalités légitimes poursuivies par le responsable du traitement.

<sup>130</sup> Le premier dit « Groupe des sages » créé par l'article 29 de la directive reprend des délégués des autorités nationales. Son activité est considérable.

base aux acteurs et opérations de communications électroniques qu'elles soient assurées par le réseau Internet ou non, qu'elles empruntent le réseau téléphonique, de câblodistribution ou hertzien. L'utilisation des données de trafic et de localisation est sévèrement réglementée de même que les communications non sollicitées et l'envoi de logiciels espions ou cookies. La Commission se voit octroyée le droit de fixer des normes techniques relatives aux appareils de communication pour lutter contre des pratiques « privaticides ».

La mise à charge d'une obligation pour les fournisseurs de services de communication, de conservation<sup>131</sup>, des données de trafic et de localisation à des fins de recherche policière a fait l'objet de lourds débats au lendemain du cauchemar du 11 septembre 2001<sup>132</sup>. La directive du 15 mars 2006<sup>133</sup> impose aux fournisseurs de services de communication de conserver ces données et à collaborer avec les autorités policières ou judiciaires, créant des risques de recherche proactive et des détournements de finalités de cette conservation<sup>134</sup>.

Au-delà de ces textes, la Charte européenne des droits fondamentaux distingue en ses articles 7 et 8<sup>135</sup> deux concepts qui, certes, peuvent se compléter et se recouper mais dont l'extension n'est pas semblable. L'article 7 évoque dans l'esprit de la Convention de 1950, le respect de la vie privée et familiale du domicile et des communications. L'article 8 énonce le droit à la protection des données à caractère personnel, épingle les limitations au traitement en même temps que les droits subjectifs essentiels de la personne concernée et souligne le rôle de l'autorité indépendante dans le contrôle du respect de ces règles. Cette **consécration quasi constitutionnelle** de la protection des données comme un principe distinct de celui de la vie privée doit être soulignée.

Relevons la caractéristique essentielle de l'approche européenne. Les données à caractère personnel ne constituent pas de simples valeurs marchandes, elles sont régies par des règles de droit public dont le but est en définitive la protection des libertés et, de manière plus essentielle encore, de la dignité humaine qui ne peut survivre que si est assurée à chaque personne une maîtrise suffisante de son

---

<sup>131</sup> Il est à noter que la Convention « Cybercriminalité » du Conseil de l'Europe prévoyait certes la possibilité pour les autorités judiciaires de demander, au cas par cas, la communication en temps réel des données de trafic et leur conservation pendant un délai maximum de 3 mois.

<sup>132</sup> A propos des initiatives réglementaires américaines et de leur influence en Europe, lire Y. POULLET - V. PEREZ, *art. cité*, J.T.D.E., 2004, p. 266 et s

<sup>133</sup> Directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006 sur la conservation des données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications et modifiant la directive 2002/58/CE, JO. L 105 du 13.04.2006 p. 54. Cette décision cadre est à analyser au regard du Protocole additionnel de 1983 du Conseil de l'Europe portant sur la même matière et analysée infra.

<sup>134</sup> Sur ce point, on note une tentative de l'Union européenne d'harmoniser les règles en matière de conservation des données de trafic à travers une proposition de décision cadre sur la conservation des données en date du 28 avril 2004.

<sup>135</sup> Ces articles de la charte sont intégralement repris dans le projet de Constitution européenne aux articles II,67 et II 68.

environnement afin qu'il puisse exprimer ces choix, la relation de la personne avec ces données nominatives ne peut donc s'assimiler à une relation de propriété mais doit tenir compte des limites imposées par le fait qu'au delà de toute information nominative, il est question de libertés et d'une conception du respect dû à la dignité de l'individu considérée comme personne<sup>136</sup>. Ainsi, curieusement, les législations de protection des données ne consacrent pas une maîtrise totale de l'individu sur « son » information. « *La liberté qui découle de la dignité humaine n'est pas une liberté robinsonienne* », comme le note Meulders-Klein<sup>137</sup> à la suite des commentateurs de la Constitution allemande qui consacre le droit à l'autodétermination<sup>138</sup>. Cette affirmation explique l'originalité de l'approche européenne par rapport à celle américaine<sup>139</sup>. Elle se traduit en particulier premièrement par la nécessité d'un examen de la légitimité de tout traitement des données ; deuxièmement, par le rôle du consentement, condition nécessaire mais non suffisante de la légitimité d'un traitement ; troisièmement, par l'importance de l'autorité de contrôle, quatrièmement par le rôle certain mais limité de l'autorégulation

### **Sous-Titre III : Des cybercrimes à définir et des règles de procédure pénale à revoir profondément.**

Le Conseil de l'Europe par la fameuse convention "Cybercriminalité"<sup>140</sup> et son

---

<sup>136</sup> Sur cette relation fondamentale entre vie privée et dignité humaine, lire J.H REICHMANN, « *The right to privacy* », in *Philosophical Dimensions of Privacy*, F.D . Schoeman ( ed.), 1984, p. 272.

<sup>137</sup> M.T. MEULDERS-KLEIN, art.cité, p. 314.et les références citées

<sup>138</sup> L'article 2.1 de la Constitution consacre le "droit de chacun au libre épanouissement de sa personnalité ». ce droit doit être lu en référence à l'article 1.1 qui affirme « *la dignité intangible de l'être humain comme principe universel* ».

<sup>139</sup> On notera que tous les auteurs américains ne partagent pas ce que nous qualifions un peu rapidement comme étant l'approche américaine. Ainsi, on note les remarques de 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 tat 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 tat insulate personal data from the observation of different parties.* »

<sup>140</sup> CONVENTION du Conseil de l'Europe sur la cybercriminalité, Budapest, 23 novembre 2001.

protocole additionnel en matière de messages pornographiques ou racistes<sup>141</sup>, documents ouverts à la signature et à la ratification d'Etats y compris non européens, tente, avec succès, d'harmoniser d'une part la liste des infractions dites de cybercriminalité et d'autre part, les règles procédurales propres à lutter contre les particularités des infractions commises par ou grâce à l'ordinateur.

Des infractions nouvelles ont vu le jour dans notre code pénal lié aux systèmes d'information d'une part et d'autre part au contenu véhiculé. Vis à vis des infractions concernant les systèmes d'information, la Convention définit tout en laissant des marges de manœuvre aux pays lors de leur ratification de la Convention, le hacking, le faux, la fraude ou le sabotage informatique. En ce qui concerne le contenu, la Convention réprime les infractions au droit de propriété intellectuelle et les messages illicites notamment pédophiles. Par un protocole additionnel<sup>142</sup>, le Conseil de l'Europe a ajouté à la liste des messages illicites, l'incitation à la haine et à la xénophobie. Il s'agit chaque fois de prendre la mesure de la spécificité d'infractions difficiles à ranger dans les infractions traditionnelles tout en respectant avec quelques entorses diront les spécialistes, le principe de neutralité technologique qui entend que ce qui est puni « *off line* » le soit aussi « *on line* ».

Du côté de la procédure pénale<sup>143</sup>, la difficulté était tout aussi grande. Comment concevoir la saisie de l'information immatérielle par essence alors que le droit traditionnel de la saisie ne s'occupe que de choses matérielles? Comment concevoir la perquisition dans des systèmes où l'information est volatile et qui se caractérisent par leur opacité? Cette dernière caractéristique des systèmes d'information conduit le législateur à prévoir des obligations de coopération à charge de toute personne qui puisse aider les services de police à pénétrer les boîtes noires que constituent les ordinateurs.

---

<sup>141</sup> PROTOCOLE additionnel à la convention sur la cybercriminalité relatif à l'incrimination de certains actes de nature raciste ou xénophobe commis par le biais de systèmes informatiques, 28 janvier 2003

<sup>142</sup> PROTOCOLE additionnel à la convention sur la cybercriminalité relatif à l'incrimination de certains actes de nature raciste ou xénophobe commis par le biais de systèmes informatiques, 28 janvier 2003

<sup>143</sup> Voir notamment, Lignes directrices sur la coopération entre les services de répression et les fournisseurs de services, 2 avril 2008, disponible sur le site [http://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/cy\\_activity\\_interface2008/567\\_prov.d.guidelines\\_provisional2\\_3April2008\\_fr.pdf](http://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/cy_activity_interface2008/567_prov.d.guidelines_provisional2_3April2008_fr.pdf).

L'Union européenne<sup>144</sup> sur la lancée de la Convention du Conseil de l'Europe approfondit la coopération entre services de police, harmonise les critères de loi et juridiction applicable en définissant de manière large les critères de rattachement d'une infraction à un territoire donnée et précisent les éléments de chaque type d'infractions. La responsabilité des personnes morales est retenue en matière de criminalité informatique.

L'Europe, à la veille d'abandonner ses piliers et nonobstant les contraintes que représente l'adoption de textes en la matière, conduit une politique résolue de coopération policière et judiciaire et se dote des moyens d'assurer une lutte efficace contre la criminalité, à laquelle elle assimile de plus en plus l'immigration sauvage. On cite ainsi, les accords de Schengen à propos du passage des frontières<sup>145</sup> ou VIS à propos des procédures et de l'octroi des visas<sup>146</sup>, la coopération menée au sein d'Europol et d'Eurojust<sup>147</sup>. La décision cadre relative à la protection des données et la coopération policière et judiciaire déjà évoquée<sup>148</sup> achève la construction d'un cadre qui cherche à concilier les impératifs de vie privée et de sécurité tout en favorisant l'interopérabilité des systèmes et en affirmant le principe de "disponibilité" des

---

<sup>144</sup> Cf. notamment, Décision cadre 2005/22/JAI du 24 février 2005 à propos des attaques contre les systèmes d'information

<sup>145</sup> Règlement n°1987/2006 du Parlement européen et du Conseil du 20 décembre 2006 sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen de 2<sup>ème</sup> génération (SIS II), *JOUE L* 381, 28/12/2006, dite « législation SIS II 1<sup>er</sup> pilier »

Décision 2007/533/JAI du Conseil du 12 juin 2007 sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen de 2<sup>ème</sup> génération, *JOUE L* 205, 07/08/2007

Sur les accords SCHENGEN I et II, lire S.K. KARANJA, *Schengen Information System and Border Control Cooperation : A transparency and Proportionality Evaluation*, Thèse, Faculté de droit d'Oslo, Juin 2006, publié par le Raoul Walhenberg Institute Human Rights Library, M. Nijhoff, Leiden, 2008.

<sup>146</sup> Décision du Conseil 2008/633/JAI du 23 juin 2008 concernant l'accès en consultation au système d'information sur les visas (VIS) par les autorités désignées des États membres et par l'Office européen de police (Europol) aux fins de la prévention et de la détection des infractions terroristes et des autres infractions pénales graves, ainsi qu'aux fins des enquêtes en la matière, *JOUE L* 218, 13/08/2008.

<sup>147</sup> La création d'Europol a été prévue par le traité de Maastricht sur l'Union européenne du 7 février 1992. Installé à La Haye, aux Pays-Bas, l'Office a démarré ses activités le 3 janvier 1994. Alors connu sous le nom de «unité "Drogues Europol"» (EDU), il limitait son action à la lutte contre la drogue. Progressivement, d'autres domaines importants de la criminalité lui ont été confiés. Le mandat d'Europol a été étendu le 1<sup>er</sup> janvier 2002 à toutes les formes graves de la criminalité internationale visées à l'annexe de la convention Europol

.En ce qui concerne Eurojust, voir la Décision 2002/187/JAI du Conseil du 28 février 2002 instituant Eurojust afin de renforcer la lutte contre les formes graves de criminalité, *JOUE L* 63, 06/03/2002. Cette unité, qui est dotée de la personnalité juridique, est composée d'un membre national par pays de l'Union, ayant qualité de procureur, de juge ou d'officier de police.

<sup>148</sup> Décision-cadre 2008/977/JAI du Conseil du 27 novembre 2008 relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale, *JOUE L* 350, 30/12/2008

données policières et judiciaires entre les autorités policières et judiciaires européennes. Tout ceci contribue à la création d'"un espace européen de liberté, de sécurité et de Justice"<sup>149</sup>. Les attentats de New York du 11 septembre 2001 mais également ceux de Madrid et Londres sont sans doute la cause. La multiplication des textes réglementaires ayant pour objectif d'assurer la sécurité tant de l'Etat que de ces citoyens est un fait incontestable.

#### **Sous-Titre IV. Des contenus à protéger par les droits de propriété intellectuelle et les droits voisins : de l'affirmation aux doutes**

L'analyse des tendances européennes en la matière révèle une hésitation entre deux volontés : celle, d'une part, d'assurer une protection maximale de l'investissement et cela, au-delà du domaine traditionnel protégé par le droit de la propriété intellectuelle ; celle, d'autre part, de maintenir un système juridique de protection conforme à la façon dont les paradigmes traditionnels du droit de la propriété intellectuelle assurent une balance équitable entre les intérêts, d'une part, des « auteurs » ou de leurs « ayants droits » et, d'autre part, des utilisateurs de l'œuvre voire de la communauté en général.

La directive 96/9/CE sur la protection juridique des bases de données du 11 mars 1996<sup>150</sup> participe certes de la première tendance. Elle crée un droit « sui generis » à la protection des données dont il est reconnu qu'elles ne peuvent être objet du droit d'auteur. On sait combien la littérature américaine s'est insurgée contre cette déviance européenne qui protège clairement l'investissement et non plus la création intellectuelle.

La même tendance présente dans la directive 98/84/CE du 20 novembre 1998 sur la protection juridique des services d'accès conditionnel<sup>151</sup> comme la télévision

---

<sup>149</sup> Sur tous ces points, le lecteur se référera à l'article de F. Dumortier, C. Gayrel, J. Jouret, D. Moreau et Y. Pouillet, La protection des données dans l' « Espace européen de liberté, de sécurité et de justice » : au-delà d'une érosion du principe de finalité, un affaiblissement des règles de protection des données. JTDE, 2009, à paraître.

<sup>150</sup> Directive 96/9/CE concernant la protection juridique des bases de données, J.O. L. 77 du 27 mars 1996, p. 20. Sur la protection « sui generis » des bases de données offertes par cette directive, lire A. LUCAS, *Droit d'auteur et numérique*, [Droit@Litec](#), Paris, 1998,

<sup>151</sup> JOCE, L.320, 28 nov. 1998, p. 54

payante mais également tout service multimédia accessible sur la base d'une autorisation individuelle et dont l'accès est protégé par des systèmes techniques tel l'encryptage. Cette directive prévoit, indépendamment de toute protection légale du contenu ainsi réservé, que les mesures techniques de protection constituent en elles-mêmes un objet digne de protection. Ainsi, la protection technique devient source d'une protection juridique d'une œuvre en elle-même non nécessairement protégeable légalement et permet d'assurer le contrôle de l'accès à l'œuvre<sup>152</sup>. Enfin, le Parlement se prépare à voter la modification de la directive de 1996 et renforcer encore les sanctions pénales et la coopération policière européenne en cas de violation des droits de propriété intellectuelle<sup>153</sup>.

A l'inverse de cette tendance qui satisfait certes les lobbies des prestataires de services de la société de l'information et, de manière plus vaste, les promoteurs du marché de l'édition technologique, d'autres textes se révèlent plus soucieux de l'intérêt d'une meilleure circulation des œuvres et programmes. Ainsi, une résolution du Parlement européen en date du 22 octobre 1998 prône clairement le soutien aux logiciels libres et aux plates-formes ouvertes et interopérables<sup>154</sup>. Plus récemment, on souligne que la directive du Parlement et du Conseil, adoptée le 9 avril 2001<sup>155</sup> à la suite de débats longs et difficiles, directive sur les droits d'auteur et droits voisins dans la société de l'information, a finalement consacré le droit des Etats membres de prévoir des exceptions aux monopoles de l'auteur (droit de reproduction ou de communication au public). Ces exceptions certes proposées de manière optionnelle, peuvent être justifiées par l'utilisation privée, à des fins de recherche, de citation, de journalisme, etc. La directive limite dans le même sens la

---

<sup>152</sup> En particulier, l'article 6 de la directive européenne sus-nommée. Cf. sur ce point déjà l'article 11 du Traité de l'OMPI sur le droit d'auteur du 20 décembre 1996. Sur cette tendance à une surprotection des œuvres sur Internet, M. VIVANT, « L'irrésistible ascension des droits de propriété intellectuelle ? » in *Mélanges Mouly*, LITEC, Paris, 1998, p. 441 ; B. HUGENHOLTZ, Copyright, Contract and Technology, What will remain of the Public Domain ?, in « *Le droit d'auteur, un contrôle de l'accès aux œuvres* », Cahier du CRID, n° 18, Bruxelles, Bruylant, 2000, p. 50 et s.

<sup>153</sup> Proposition amendant la Directive du 26 avril 2006 relatives aux mesures pénales pour assurer l'effectivité des droits de propriété intellectuelle en cours de discussion.

<sup>154</sup> Cette résolution fait suite au Livre Vert de la Commission (COM (97)263) du 3 décembre 1997 relatif à la convergence des secteurs de télécommunications, media et technologies de l'information et ses implications pour la régulation.

<sup>155</sup> Directive 2001/29/CE du 22 mai 2001, sur l'harmonisation de certains aspects du droit d'auteur et des droits voisins dans la société de l'information, JOCE 22 juin, n° 1, 167, p. 10.

protection que pourraient apporter des mesures techniques<sup>156</sup>.

Il reste, il est vrai, à chaque Etat à inscrire dans sa législation nationale de telles réserves et d'assurer ainsi que la balance traditionnelle que les législations relatives au droit d'auteur garantissent entre les intérêts légitimes des créateurs (ou de leurs ayants droit) et ceux de la société de la société au profit de certains acteurs comme la recherche, l'éducation, la presse, etc. La question de la copie privée et la lutte contre les télé-déchargements illicites<sup>157</sup> a fait l'objet de discussions parlementaires européennes aigües suite aux débats français relatifs à la loi HADOPI<sup>158</sup>, déclarée depuis anti constitutionnelle et modifiée. Ainsi le Parlement européen<sup>159</sup> rappelle à la suite du SMSI que l'accès à Internet et au savoir représente un droit pour tous dans nos sociétés de l'information et que nul ne peut en être privé sans les fortes garanties d'une procédure judiciaire : « (...) *considérant que l'analphabétisme informatique sera l'analphabétisme du XXI<sup>e</sup> siècle ; considérant que garantir l'accès de tous les citoyens à Internet équivaut à garantir l'accès de tous les citoyens à l'éducation et considérant qu'un tel accès ne devrait pas être refusé comme une sanction par des gouvernements ou des sociétés privées ; considérant que cet accès ne doit pas faire l'objet d'abus aux fins d'activités illégales ; considérant qu'il est important de se pencher sur les questions émergentes telles que la neutralité des réseaux, l'interopérabilité, l'accessibilité globale de tous les nœuds d'Internet et l'utilisation de formats et de normes ouverts, (...)* », le Parlement européen recommande au Conseil de « (...) *procéder à l'adoption de la*

---

<sup>156</sup> Sur les limites à imposer aux protections qu'apportent les mesures techniques, lire S. DUSOLLIER, Y.

POULLET, M. BUYDENS, Rapport au 3<sup>ème</sup> colloque « Infoéthique » de l'UNESCO, disponible sur le site du CRID : <http://www.crid.ac.be>. Voir aussi, le document de travail on electronic copyright management systems (Feb. 24, 2000): How to balance the benefits and the risks linked with these technologies

<sup>157</sup> Ces discussions parlementaires ont été initiées suite à une consultation de la Commission (Commission Consultation on fair compensation for acts of private copying (Feb. 2008))

<sup>158</sup> La **loi Hadopi** ou loi **Création et Internet**, « Loi n°2009-669 du 12 juin 2009 favorisant la diffusion et la protection de la création sur internet », est une loi française qui sanctionne le partage de fichiers en pair à pair en tant qu'infraction au droit d'auteur. La récidive est punie de manière croissante et le législateur parle de « riposte graduée ». Cette loi crée une « Haute autorité pour la diffusion des œuvres et la protection des droits sur Internet » (Hadopi), organisme indépendant français de régulation

<sup>159</sup> Le 10 avril 2008, une résolution (Résolution du Parlement européen du 10 avril 2008 sur les industries culturelles en Europe (2007/2153(INI), 10 avril 2008) a été adoptée par le parlement européen à 314 voix contre 297, enjoignant les états membres à « reconnaître qu'Internet est une vaste plate-forme pour l'expression culturelle, l'accès à la connaissance et la participation démocratique à la créativité européenne, créant des ponts entre générations dans la société de l'information, et, par conséquent, à éviter l'adoption de mesures allant à l'encontre des droits de l'homme, des droits civiques et des principes de proportionnalité, d'efficacité et d'effet dissuasif, telles que l'interruption de l'accès à Internet. »

*directive concernant des mesures pénales visant à l'application des droits de propriété intellectuelle, suite à une évaluation, à la lumière des recherches actuelles en matière d'innovation, du degré de nécessité et de proportionnalité et tout en interdisant, en vue de cet objectif, le contrôle et la surveillance systématiques de toutes les activités des utilisateurs sur Internet et en veillant à ce que les sanctions soient proportionnées aux infractions commises; dans ce contexte, respecter la liberté d'expression et d'association des utilisateurs individuels et lutter contre les incitations aux cyber-violations des droits de propriété intellectuelle, y compris certaines restrictions d'accès excessives imposées par les titulaires de droits de propriété intellectuelle eux-mêmes ; (...) »*

On relève également, le débat difficile en cours depuis des années au Parlement européen à propos de la brevetabilité des logiciels où il semble que les députés élus remettent en cause l'approche favorable retenue par leurs prédécesseurs<sup>160</sup>. Sans doute faut-il y voir la crainte du Parlement de voir l'innovation technologique largement immatérielle dans le cadre des programmes d'ordinateur, confisqué grâce au brevet conçu pour d'autres finalités et d'autres types d'inventions plus techniques.

Les limites de la protection des contenus de l'Internet ainsi tracées, c'est très légitimement que les instances européennes adoptent les mesures nécessaires pour une protection juridique plus efficace par une meilleure coopération entre les administrations en charge de la détection et de la répression des actes de piratage ou de contrefaçon<sup>161</sup>.

## **Conclusions**

L'introduction s'interrogeait sur le rôle du droit face aux technologies de l'information et de la communication. Le droit tel qu'on l'entend traditionnellement, c'est-à-dire l'expression des choix normatifs d'une société nationale souveraine,

---

<sup>160</sup> A ce propos, le vote massif intervenu le 2 février 2005 au Parlement européen demandant à la Commission de revoir la proposition de directive du 20 fév. 2002 (J.O. 25 juin 2002, C 151 E/129) sur la brevetabilité des inventions liées à l'ordinateur.

<sup>161</sup> Cf. récemment le document de travail de la Commission du 14 février 2002 (COM 2004, 261, final). Directive 2004/48/CE du 29 avril 2004 relative à la mise en œuvre des droits de propriété intellectuelle (JO, 30 avril 2004, L 157/45).

n'était-il pas condamné, à l'heure de l'Internet ? La réponse apportée atteste certes de l'existence d'autres formes de régulation présentes dans la société de l'information et avec lesquelles le droit est désormais forcé de composer voire de trouver des alliances. Par ailleurs la souveraineté ne peut plus se concevoir au niveau des Etats - nation mais au sein d'entités régionales. La dimension internationale de l'Internet exige le développement d'un droit international de l'Internet qui ne peut être l'adoption d'un plus petit commun dénominateur entre les peuples mais doit permettre, par l'instauration d'un dialogue entre les diverses parties prenantes de cette société de l'information, de définir les bases d'une société de l'information accessible à tous et respectueuse de valeurs essentielles<sup>162</sup>. Au-delà de la création d'« autorités » réellement indépendantes<sup>163</sup> qui se multiplient pour réguler le secteur des médias, pour arbitrer les conflits entre libertés et intérêt de l'entreprise ou intérêt général ou plus généralement remplacer sur l'Internet nos juridictions officielles, l'Etat veillera également à mettre en place des lieux de discussion sur l'impact des technologies nouvelles sur nos sociétés et sur l'humain. Il y invitera selon le vœu du SMSI tous les acteurs et intéressés sans en oublier.

L'intervention du droit dans divers domaines n'est pas dictée par le seul fait technologique. Elle s'inscrit au contraire dans un dialogue avec les acteurs du développement technologique. Il s'agit tantôt - l'exemple de la signature électronique le montre - de rappeler les exigences que le droit véhicule à travers ses concepts, tantôt - l'exemple des exceptions en matière de droit d'auteur en témoigne - d'exiger que le développement technologique s'opère en conformité avec les équilibres mis en place par les législations traditionnelles. Si certains

---

<sup>162</sup> Ce besoin d'instruments internationaux en particulier en matière de protection des données a fait l'objet de deux déclarations des autorités francophones de protection des données. Aini, la déclaration de Ouagadougou, 27 novembre 2004 (point 51) : « *Nous sommes convenus d'attacher une importance particulière à la protection des libertés et droits fondamentaux des personnes, notamment de leur vie privée, dans l'utilisation des fichiers et traitements de données à caractère personnel. Nous appelons à créer ou consolider les règles assurant cette protection. Nous encourageons la coopération internationale entre les autorités indépendantes chargées dans chaque pays de contrôler le respect de ces règles.* » et la déclaration de Bucarest, 28 septembre 2006 (point 59) : « *Nous appelons à l'intensification des travaux nécessaires à l'adoption de législations et réglementations assurant la protection des personnes, de leurs libertés et de leurs droits fondamentaux dans l'utilisation des fichiers et traitements de données à caractère personnel, et, conscients de l'accroissement de la circulation de données personnelles au-delà des frontières, marquons notre intérêt pour examiner l'opportunité d'élaborer un instrument international garantissant, dans ces circonstances, le droit des personnes à la protection des données à caractère personnel, tout en tenant compte de nos objectifs légitimes en matière de lutte contre le crime, la corruption et le terrorisme* » ;

<sup>163</sup> Sur ces autorités, la nécessité de leur indépendance vis-à-vis de l'exécutif et du gouvernement et leur rôle précieux dans la défense des libertés, lire

développements technologiques affectent nos libertés, sans doute, le droit se doit-il d'intervenir, de contraindre la technologie à trouver en elle-même les solutions adéquates voire d'affirmer de nouveaux droits aptes à corriger les déséquilibres sociétaux nouveaux créés par ces développements. Ainsi, s'expliquent les droits nouveaux apportés par les législations dites de protection des données personnelles ou l'affirmation d'un droit « universel » à l'accès à certains services de la société de l'information.

Quelques mots ou idées clés paraissent par ailleurs caractériser l'intervention du droit. J'en évoque quatre.

- Le premier est certes l'affirmation sans détour du **droit d'accès universel** à l'Internet et au savoir qu'il véhicule. Le Sommet mondial de la Société de l'Information le conçoit de manière large : accès à l'infrastructure, à l'éducation et aux ressources publiques informationnelles. Le même souci est exprimé par le Parlement européen qui à propos de la lutte contre la copie privée rappelle avec force le droit de chacun à accéder à l'Internet et à s'y exprimer librement. Le Conseil de l'Europe va jusqu'à affirmer la valeur de service public de l'Internet et y consacrer une Recommandation<sup>164</sup>.
- La **neutralité** face à la technologie voire l'équivalence fonctionnelle des solutions technologiques face aux solutions traditionnelles constitue une autre constante du droit. Nous l'avons vu appliquer en matière de droit des contrats, de la criminalité informatique voire de droits d'auteurs.
- La **proportionnalité** est omniprésente pour apprécier les limites de l'utilisation des TIC face aux risques encourus par notre vie privée ; elle constitue également

---

<sup>164</sup> [Recommandation CM/Rec\(2007\)16](#) du Comité des Ministres aux Etats membres sur des mesures visant à promouvoir la valeur de service public de l'Internet, adoptée le 7 novembre 2007 rappelé encore récemment par la recommandation à propos des Filtres sur l'Internet (Recommandation CM/Rec(2008)6 du Comité des Ministres aux Etats membres sur les mesures visant à promouvoir le respect de la liberté d'expression et d'information au regard des filtres internet, 26 mars 2008) : « Conscient de la valeur de service public de l'Internet, comprise comme étant le fait pour les personnes de compter de manière significative sur l'Internet comme un outil essentiel pour leurs activités quotidiennes (communication, information, savoir, transactions commerciales, loisirs) et de l'attente légitime qui en découle que les services de l'Internet soient accessibles et abordables financièrement, sécurisés, fiables et continus, et rappelant sur ce point la Recommandation Rec(2007)16 du Comité des Ministres sur des mesures visant à promouvoir la valeur de service public d'Internet »

le critère par lequel les conflits entre libertés peuvent se régler, voire les exceptions à ces libertés se mesurer.

- Enfin, comment ne pas voir que l'obsession de la **sécurité** conduit le droit à intervenir à la fois lorsqu'il s'agit de protéger les investissements immatériels qui circulent sur le Net, lorsqu'il s'agit de protéger les transactions et leur paiement et enfin lorsqu'il s'agit de la société elle-même au risque de nos vies privées ?

En définitive, si le droit se trouve bousculé par la technologie, il n'en est pas moins bien vivant. Au terme de la réflexion proposée, il importe de souligner le rôle de nos assemblées législatives d'instaurer le débat que l'impact des technologies rend chaque jour plus nécessaire : « Quelle société voulons-nous ? ». Sans se hâter, sans se laisser imposer ni la loi du marché, ni la loi de la technologie mais en les ayant comprises et en dialogue avec elles, les législateurs de nos assemblées démocratiques, sans doute forts de leur coopération, se doivent de définir de nouvelles lois qui ne soient pas des contraintes au développement et à l'innovation mais garantissent une technologie respectueuse de nos libertés. Par la création de nouveaux lieux de dialogue en dehors des enceintes parlementaires et y recherchant non sans hésitation et parfois avec précipitation de nouveaux consensus, le droit incarné par la loi accomplit sa fonction traditionnelle qui est la recherche du juste, le respect des libertés et le développement de tous.