Comment appliquer les règles de protection des données aux transferts de données personnelles dans une société à la fois globale mais également multi-économique et multiculturelle ?

Yves Poullet*

Lex Electronica, vol. 12 n°1 (Printemps / Spring 2007)

http://www.lex-electronica.org/articles/v12-1/poullet.htm
http://www.lex-electronica.org/articles/v12-1/poullet.pdf

---

*(**Note** : Cet article reprend une allocution présentée lors de la Conférence organisée conjointement par l'US Department of Commerce et le Groupe de l'article 29 – Bruxelles, Centre Borschette, les 23 et 24 octobre 2006)*

Monsieur le Président

1. Voilà la question pour laquelle vous me faites l'honneur de me demander comme professeur d'Université, autorité indépendante s'il en est, quelques pistes de réflexion.

La question trahit pour le moins un certain embarras ou, en tout cas, l'affirmation de deux volontés apparemment contradictoires, celle, d'une part, d'assurer « globalement » les valeurs que le régime de protection des données incarne, globalement, c'est à dire sans considération de frontières mais, d'autre part et dans le même temps, la volonté de ne pas heurter la diversité des réalités économiques et culturelles qui se côtoient et de plus en plus se heurtent dans notre société globale de l'information. Désormais, en effet, nulle culture nationale, nulle économie ne sont plus à l'abri de leurs frontières naturelles.

La question que vous me posez est pour le moins pertinente. Récemment, mon équipe namuroise s'intéressait à la protection des données en Inde. Il nous fut répondu par des spécialistes indiens de la « Data Protection » que l'Inde disposait d'une législation « l'Information Security Act » qui, depuis 2000, veille à la sécurité des données et accorde aux bases de données une entière protection juridique. Cette difficulté de dialogue et de compréhension mutuelle témoigne de l'impossibilité d'imposer en tant que telle un concept qui pour nous, Européens, est devenu l'objet, au-delà d'une simple sensibilité culturelle, d'un véritable droit de l'Homme. L'exigence de permettre à chacun d'assimiler ce souci de protection des données et ce, selon son génie propre et son propre système normatif sans trahir l'objectif poursuivi par ce concept nous paraît évidente. Comment permettre cette diversité d'approches sans trahir les valeurs que nous attachons à la protection des données ?

Enfin, la question est posée dans le contexte particulier de la réunion de ce jour, celui d'un dialogue entre les Etats-Unis et l'Europe, un dialogue que des événements récents ont mis à l'épreuve et sur lesquels nous dirons quelques mots. Nonobstant ces divergences, votre présence aujourd'hui témoigne en tout cas d'une conviction et d'une foi partagée en la cause qui nous réunit.

---

* Directeur du Centre de Recherche en Informatique et Droit (CRID - http://www.crid.be), Facultés Universitaires Notre-Dame de la Paix, Namur, Belgique. Professeur à la faculté de droit de Namur et de Liège. Courriel : yves.poullet@fundp.ac.be.

2. En réponse, notre propos rappelle tout d'abord comment l'Europe a progressivement consacré et interprété ce droit de l'Homme qu'est la protection des données à caractère personnel. Ces consécration et interprétation dynamiques expliquent l'attitude de l'Union Européenne, héritière de la Convention du Conseil de l'Europe (la CEDH).

Ce rappel nous permettra dans un deuxième temps de comprendre comment, en 1995, à une époque où Internet balbutiait encore de ce côté-ci de l'Atlantique, l'Union européenne a envisagé la question de la réglementation des flux transfrontières. Progressivement, au travers de multiples décisions et grâce à l'impulsion du groupe dit de l'article 29, elle a développé un véritable système complet, cohérent et ouvert des différentes méthodes par lesquelles une protection adéquate peut être offerte lors de transfert de données en dehors des territoires de l'Union européenne.

Ce système patiemment mis en place semble aujourd'hui ne répondre que de manière incomplète à la réalité des flux transfrontières. Trois raisons seront évoquées et développées. Elles nous amènent en conclusion à plaider pour la nécessité de trouver, à partir du dialogue entre nos deux continents, l'amorce d'une solution globale affirmant pleinement l'intérêt de chaque « *Netizen* » à voir protéger ces données à caractère personnel et garantissant le respect de cet intérêt.

I. De l'article 8 CEDH au régime européen des Flux Transfrontières de Données (FTD)

3. L'origine du régime européen de protection des données est connue. La Convention Européenne des Droits de l'homme proclame dès 1950 en son article 8 la protection de la vie privée et familiale comme un des droits fondamentaux de l'homme.

On sait l'interprétation que la Cour de Strasbourg a donnée à ce droit fondamental et les conséquences qu'elle en a tirées.

Trois réflexions à ce propos :

- La Convention, répète à l'envie la Cour de Strasbourg, est un instrument vivant, dynamique dont l'interprétation ne peut se concevoir que dans le sens d'une extension des concepts (*one-way interpretation*). Ainsi, la protection de la « vie privée-intimité » face à l'Etat, conception négative marquée par une interdiction de traiter des données dites sensibles et de lever le secret de la correspondance fait place à une approche plus positive, celui du droit à l'autodétermination informationnelle. Ce droit entend assurer à chacun la maîtrise de la circulation « légitime » de son image informationnelle. Il s'entend de la protection de toutes les données à caractère personnel et vise aussi bien l'Etat que le secteur privé. La Convention n° 108 du Conseil de l'Europe de 1981 sur la protection des donnés à caractère personnel et, à sa suite, la directive 95/46/CE du 24 octobre 1995 consacre cette évolution.
- La jurisprudence rappelle que le droit à la protection des données ne peut rester théorique mais suppose l'adoption de mesures concrètes et effectives de protection.
- Enfin, la jurisprudence strasbourgeoise insiste – et sans doute ce point distingue américains et européens – sur l'obligation positive de l'Etat d'assurer la protection de ce droit. Cette affirmation justifie tant l'intervention législative, la mise sur pied d'autorités indépendantes de protection des données que les règles relatives aux flux transfrontières. La protection des droits de l'homme ne peut en effet s'arrêter aux frontières sous peine de devenir ineffective. Il est clair que pour l'Europe, la protection des données ne peut être laissée aux seules forces du marché.

4. L'Union européenne reconnaît depuis le traité d'Amsterdam l'héritage de la Convention européenne. Ainsi, la Convention et donc son article 8 sont considérés comme un instrument constitutionnel de l'ordre public européen, en même temps qu'il lui est reconnu une priorité vis-à-vis de toutes les autres normes nationales et internationales, y compris celle de l'OMC.

En faisant suite à l'évolution de la jurisprudence strasbourgeoise, la Charte européenne des Droits de l'Homme adoptée à Nice, embryon de la Constitution européenne a consacré le droit à la protection des données comme un droit autonome par rapport à celui de la vie privée. La protection de ce droit doit être mise en œuvre, dit le commentaire de la Charte, tant dans les relations internes qu'internationales.

Sur ce dernier point, on peut affirmer que les articles 25 et 26 de la directive 95/46 avait quelque peu anticipé cette reconnaissance constitutionnelle du droit à la protection des données.

Venons-en, si vous le voulez bien, à l'analyse de cette disposition.

5. Il s'agit – et les considérants de la directive l'expriment clairement – de ne pas nier la réalité, les besoins et les avantages du commerce international mais de veiller à concilier tout à la fois ce développement et la garantie du respect de la protection des données en veillant à ce qu'une protection adéquate soit offerte par les destinataires des flux transfrontières, à défaut en interdisant les flux.

Notons que le champ d'application de la directive reste purement territorial même si on ne peut en nier l'impact extraterritorial des dispositions des articles 25 et 26. Je veux dire par là que la directive vise les seules activités d'établissements situés sur le territoire de l'Union Européenne. C'est d'eux et d'eux seuls, qu'on réclame qu'ils veillent lors des flux transfrontières à s'assurer de la protection adéquate offerte par le destinataire.

6. L'article 4.1.e) contient toutefois une dérogation à ce principe de la territorialité. La directive est applicable si le responsable du traitement établi en dehors du territoire utilise (*makes use*), à des fins de traitements, un équipement situé sur le territoire d'un Etat membre. L'adoption de cette disposition, dont même les auteurs de la directive ont quelque difficulté à saisir le sens est, pour moi, prémonitoire, appliqué au contexte de nos infrastructures globales et interactives. Elle signifie que si, à partir d'un territoire hors de l'Union européenne, un responsable de traitement dispose de la pleine maîtrise du fonctionnement total ou partiel d'un terminal situé dans l'Union européenne et on songe aux « *spywares* », aux « *cookies* » et à certains programmes d'extraction à distance de données dans des bases de données européennes, il est entièrement soumis à la directive. Cet article s'applique donc aux transferts passifs dans la mesure où le transfert en cause est entièrement soumis technologiquement au bon vouloir du responsable du traitement situé à l'extérieur de l'Europe.

7. A l'inverse, les articles 25 et 26 s'appliquent aux transferts actifs de données, c'est-à-dire ceux où le responsable du traitement décide de l'envoi des données ou du moins en autorise le transfert.

La règle d'or en la matière est qu'il doit s'assurer qu'une protection adéquate soit assurée par les destinataires.

L'utilisation des mots « protection adéquate » en lieu et place des termes « protection équivalence » ou « protection suffisante » constitue une originalité de l'approche européenne. Elle implique le rejet de toute attitude a priori qui s'attacherait à la seule nature et au contenu du mode de protection offert par le destinataire.

La question n'est pas de savoir s'il existe dans le pays du destinataire, un instrument de protection de même nature qu'en Europe, en l'occurrence une loi et dont le contenu serait quasi similaire à celui de la directive, ce qui eût constitué un acte d'impérialisme européen. Il s'agit de se poser la question : « Au vu du flux en question et des risques liés aux caractéristiques de ce flux, le moyen de protection offert par le destinataire, garantit-il le respect des exigences de protection des données telles que voulues par l'Union européenne ? ». La garantie du respect doit s'examiner, rappelle le fameux « *Methodology Paper* » du Groupe de l'article 29, tant à propos du contenu de la protection offerte, qu'à propos des moyens mis en place pour s'assurer du respect de ce contenu. La constatation de la conformité de contenu n'évacue pas la nécessité de s'assurer de l'effectivité du respect de celui-ci, peu importe la nature de la réglementation choisie et les institutions ou sanctions formellement mises en place par le pays étrangers. J'insiste sur ce point au moment où les évaluations du caractère adéquat me semblent parfois basculer vers une analyse tatillonne du seul contenu et délaisse la vérification de l'effectivité.

8. Ainsi, a priori, l'Europe s'interdit tout préjugé – et nous revenons à la question initiale qui constitue l'objet de ce propos – sur la nature de la méthode de protection choisie. Des solutions d'autoréglementation (les « *Safe Harbour Principles*», les solutions contractuelles ou les Binding Corporate Rules (B.C.R.) en sont), de corégulation (le cas japonais s'appuyant sur la combinaison d'une loi, la loi de 2003, des codes de conduite et d'un système de label l'illustre) sont toutes acceptables à condition que ces solutions soient conformes et effectives.

Progressivement, avec l'aide du Groupe de l'article 29, s'est construit un véritable système des différents modes de protection qui peuvent être offerts en matière de protection des données. Ainsi, la protection offerte par le destinataire peut trouver sa source dans l'environnement « régulatoire » au sens le plus large dans lequel se meut son activité (qu'il s'agisse d'un secteur précis ou non, qu'il s'agisse de systèmes d'autorégulation, codes de conduite, label, …). Elle peut trouver sa source dans le contrat spécifique que noue l'émetteur et son destinataire à propos précisément du flux qui les concerne. Elle peut s'appuyer enfin – c'est l'innovation prometteuse des B.C. R. – sur la structure hiérarchique qui caractérise les multinationales et les modes internes de contrôle, d'audit et de sanction que ces multinationales peuvent aisément imposer.

Cette diversité des modes acceptables traduit, je le crois, la large ouverture de l'Union européenne à accepter les solutions originales mises en place dans des pays de culture différentes. Je le répète, il ne peut être question d'impérialisme européen.

9. Les discussions que vous allez avoir sur l'évolution des « *Safe Harbour Principles* » m'amènent à quelques considérations supplémentaires. Vous avez pris connaissance des conclusions publiées sur le site de l'Union européenne à propos de l'évaluation du système que la Commission a jugé, il y a 6 ans, le 26 juillet 2000, adéquat. Elles traduisent un relatif désenchantement. Cette désillusion ne remet pas en cause le choix du système des « *Safe Harbour Principles* » mais bien, son application effective. Permettez moi d'être brutal « *Self-regulation is definitively a solution but please, take it seriously* ». Ce que l'évaluation révèle est un manque de connaissance par la plupart des entreprises, qui adhèrent aux Safe Harbour, de l'exacte portée de leur engagement. Les « *Privacy Policies* » sont bien souvent des déclarations vagues sans structure, mal référées sur les sites web et c'est à la personne concernée de les découvrir et d'en comprendre la portée. Au-delà, on regrette que votre département du commerce n'impose pas une standardisation des clauses que la qualité et la portée du contrôle opéré par les ADR soient peu évidentes et on s'interroge sur la réalité des sanctions dissuasives même lorsqu'elles existent sur papier. A ce propos, l'inscription sur la liste du département du commerce devrait constituer un label susceptible de retrait en cas de

non contestation du non respect de la « *Privacy policy* ». Nos critiques s'adressent également aux autorités de contrôle européennes dans leur tâche de sensibilisation des personnes concernées, de surveillance des contenus de « *Privacy policies* ». Enfin, on déplore l'absence de visibilité du « *DPA Panel* » mis en place par les autorités européennes de protection des données pour servir de relais aux personnes concernées.

10. Au-delà de ces remarques relatives aux « *Safe Harbour Principles* », quelques réflexions sur le système mis en place par les articles 25 et 26.

Si la souplesse du système et sa prise en considération de l'originalité proposée par chaque pays voire par chaque responsable de traitement constituent les mérites essentiels de la formule, il est absolument nécessaire d'éviter toute discrimination de jugement lors de l'examen de l'adéquation des solutions concrètes mises en place. A cet égard, au niveau national, la diversité de nature des autorités en charge de l'évaluation de l'adéquation voire, dans certains pays, l'absence de tout contrôle a priori des flux transfrontières de données, constatées et relevées par le premier rapport sur l'application de la directive devraient être évitées. Même réflexion au niveau des décisions d'adéquation de la Commission dont il importe qu'elles soient motivées au regard de critères précis pour ne point être suspectées de complaisance vis-à-vis de tel ou tel système.

On ajoutera l'intérêt pour les entreprises ayant des établissements dans plusieurs pays européens à partir desquels des flux peuvent être opérés de pouvoir disposer d'un guichet unique, la solution proposée par le groupe de l'article 29 à propos des BCD devrait être étendu à l'ensemble des autres techniques.

Un dernier point mérite d'être souligné. Ne faut-il pas au gré des nouvelles directives européennes, des opinions du Groupe de l'article 29 et de la jurisprudence réévaluer les critères fixés en 1998 ?

11. Au-delà de ces critiques, une réflexion plus fondamentale nous apparaît s'imposer. Le système mis en place par les articles 25 et 26 apparaît ne point couvrir l'ensemble des flux transfrontières. Il ne s'agit pas simplement de relever que bien des pays vis-à-vis desquels des transferts s'opèrent ne disposent pas de systèmes considérés par la Commission ou par les pays comme adéquats, ainsi, pour ne citer qu'eux, l'Inde, le Japon, la Russie, la Chine vis-à-vis desquels les flux transfrontières à partir de l'Europe se multiplient.

A cet égard, il serait utile de s'interroger sur le nombre de flux couverts par une des solutions proposées par la directive au regard de l'ensemble des flux réels. Mon problème n'est pas là, il est plus fondamental. L'approche suivie par la directive en ce qui concerne les flux transfrontières est insuffisante au regard de la réalité actuelle des flux dans le contexte de notre société de l'information. En particulier, nous relevons trois insuffisances qui amènent, me semble-t-il, à analyser la façon dont le système de la directive 95/46 doit être complété.

II. Les insuffisances du système européen mis en place par la directive 95/46/CE et le besoin d'une solution globale.

12. La première raison de l'insuffisance du régime actuellement mis sur pied vient d'une décision récente du 6 novembre 2003 de la Cour européenne de justice, en cause la dame Lingvist. Une des questions analysées était la suivante : la consultation possible à partir de pays extérieurs à l'Union européenne doit-elle s'analyser comme constitutive de flux transfrontières au sens des articles 25 et 26. Les arguments avancés par les juges européens pour répondre négativement à la question posée sont de l'avis de tous les commentateurs peu convaincants. Il suffit de penser aux risques que présentent des « *sniffers* » d'adresses ou des « *search engines* », comme le mythique Google pour se rendre compte que la consultation de

sites peut présenter des dangers pour la protection des données. Qui n'a été surpris de retrouver associée à son nom, telle donnée découverte par le « *search engine* », donnée parfois oubliée par lui-même ?

Sans doute, et c'est la raison essentielle évoquée par les juges pour refuser l'application des articles 25 et 26, est-il difficile d'imaginer de régler la multitude de flux susceptibles d'être générés et ce, en direction d'un nombre indéfini de pays ? Ne pouvait-on, cependant appliquer ces articles en constatant que l'article 26.1. contient nombre d'exceptions applicables en la matière et que, par ailleurs, la liberté d'expression qu'incarne nombre de ces sites web justifient des dérogations supplémentaires. En toute hypothèse, quelques règles s'imposent en la matière de manière à éviter les risques majeurs liés à de telles consultations en certains pays lointains ou proches.

12. Le deuxième constat d'insuffisance est plus grave encore. De récentes législations américaines comme le « *Patriot Act* » et le « *SOX Act* » (le SARABANNES-OXLEY Act, à propos des obligations de signalement des employés dans les entreprises à propos de certains faits délictueux) provoquent en Europe un certain émoi, ainsi l'affaire SWIFT et ce dans la mesure où des données personnelles acheminées aux Etats-Unis dans le cadre de transferts entre entreprises peuvent se trouver saisies par les autorités publiques américaines, en contradiction avec les attentes légitimes des personnes concernées et sur base de lois sans équivalent en Europe. Cette question de la transmission par des entreprises privées à des autorités publiques étrangères dans le cadre de législation de sécurité publique n'a pas été aperçue lors de la rédaction des « *Safe Harbour Principles* » qui se contentent de noter que l'adhésion aux principes ne peut être remis en cause par les exigences de la sécurité nationale, l'intérêt public et le respect des lois des Etats-Unis.

Pour être plus précis, la décision d'adéquation sur base du premier pilier n'est pas remise en cause par une décision ultérieure de l'Etat considéré adéquat dans la mesure où cette décision s'appuie sur des raisons de sécurité nationale et peut trouver son fondement dans une loi du pays du destinataire. Cette position semble récemment avoir été remise en cause par le Groupe de l'article 29 dans son avis concernant le SOX Act, avis en date du 1er février 2006. Il s'agissait en l'occurrence de savoir dans quelle mesure une entreprise soumise à la directive ou plutôt les employés de cette entreprise étaient ou non tenus par l'obligation légale américaine de signaler les malversations et certaines infractions commises dans les domaines bancaire, de comptabilité, du contrôle interne des comptes, de l'audit, de la lutte contre la corruption et les infractions financières. Lors de cet avis, le Groupe de l'article 29 affirme sans ambages « *qu'une obligation imposée par une loi ou un règlement étrangers qui exigeraient l'établissement de systèmes de signalement ne saurait être qualifiée d'obligations légales légitimant le traitement de données dans l'UE. Toute autre interprétation permettrait à des législations étrangères de contourner les règles fixées par l'UE avec la directive 95/46/CE* ». Sans doute, s'agissait-il dans le cas d'analyser le comportement d'entreprises localisées en Europe, mais on peut à partir de là se demander quelle sera la position de ce même groupe lorsqu'il s'agira de s'interroger sur la transmission à une entreprise américaine de données dont on sait qu'elles pourraient faire l'objet d'une obligation de transmission aux autorités américaines dès leur passage de la frontière.

13. La question se trouvera en tout cas posée si, comme le souhaitent le contrôleur européen à la protection des données et le rapport ROURE au Parlement européen, la future décision cadre à prendre dans le contexte cette fois du 3ème pilier de l'Union européenne, soit celle relative à la protection des données dans le contexte relatif à la coopération policière et judiciaire en matière pénale, s'étend aux obligations de coopération avec les autorités publiques, obligations mises à charge des entreprises privées par des lois dites de sécurité

publique. Il sera alors nécessaire sur base cette fois du 3ème pilier, d'examiner le caractère adéquat des législations étrangères instaurant cette coopération vis-à-vis des règles européennes.

Ainsi, même si le flux vers un pays tiers est jugé adéquat aux yeux du premier pilier, il peut dans la mesure où la réglementation du pays tiers imposerait la communication de données à ses autorités publiques, être jugé inadéquat aux yeux du 3ème pilier. Sans doute, les entreprises n'apprécieront pas cette remise en cause qui les obligent soit à remettre en cause la continuité de l'opération économique qui justifiait le flux transfrontières, soit à ne pas respecter le « *diktat* » des pays étrangers, mais alors à s'exposer à des sanctions sur le sol étranger.

Quoiqu'il en soit, on conçoit mal que ce ne soit pas au niveau politique le plus élevé c'est-à-dire au niveau intergouvernemental que soient discutées les conséquences des réglementations de sécurité publiques prises dans un pays étranger sur le transfert des données européennes à caractère personnel y transitant ou y transférées. Il va de soi que ces discussions doivent pouvoir avoir un effet sur les décisions d'adéquation prises sur base du premier pilier.

14. La troisième considération est plus cruciale encore. L'interactivité et le caractère international des réseaux en même temps que leur utilisation dans la vie de tous les jours modifient de façon radicale la problématique des flux transfrontières.

Les articles 25 et 26 conçus avant l'ère de l'Internet ne concevaient les risques liés aux flux transfrontières qu'à propos d'opérations spécifiques de transfert entre responsables de traitement. Or, aujourd'hui la réalité est différente. Chacun d'entre nous consulte des sites à l'étranger, y laisse des traces, reçoit des sollicitations ou publicités venant de l'étranger, partage des informations ou des opinions dans des forums de discussion, autant de flux entrants et sortants de l'Union européenne non visés par la directive 95/46/CE et qui, on le sait, emportent de multiples risques pour notre vie privée.

Pour faire face à des risques liés à la nature même du réseau de l'Internet, la directive 2002/58/CE sur la « protection des données dans le secteur des communications électroniques » consacre des règles de protection de l'utilisation ou de l'abonné aux services de communications électroniques, sans plus se préoccuper des personnes visées par les obligations qu'elles créent. L'envoi de courrier non sollicité est banni peu importe que l'émetteur de ce courrier soit localisé en Europe ou à l'extérieur et dans ce dernier cas peu importe la législation qui lui est applicable (par ex. : le système de l' « *opt out* » du *Spam Act* américain), l'utilisation du réseau pour pénétrer sans consentement dans le terminal de l'internaute est interdite peu importe la nationalité et la localisation de celui qui procède à une telle intrusion, le devoir de confidentialité relatif aux messages transmis s'impose à tout opérateur ou fournisseur d'accès, sans considération du lieu de leur établissement.

De telles dispositions ont, sans nul doute, un effet extraterritorial et on peut imaginer dès lors que le respect de ses règles soit imposé à des entreprises non localisées en Europe sous peine de blocage de l'accès à leurs sites ou autres sanctions possibles.

Peut-on les considérer ces règles, comme incompatibles avec les règles de l'OMC ?

15. Nous pensons que non. Nous nous appuyons pour cela sur la décision de l'organe d'appel de l'OMC prononcé le 7 avril 2005 dans une affaire opposant les Etats-Unis et Antigua. Cette décision est la première de l'OMC en ce qui concerne l'Internet et la première à mettre en évidence les conséquences de l'exception d'ordre public consacré par les GATS. En bref, la législation américaine du « *Wire Act* » soumettait les jeux et paris sur l'Internet à des obligations administratives et réglementaires, ce qui avait pour effet de restreindre

significativement la possibilité pour les serveurs de tels sites d'offrir leurs services aux Etats-Unis.

L'organe d'appel donne raison aux Etats-Unis en considérant que, nonobstant la portée extraterritoriale des règles adoptées et leur indiscutable impact sur le commerce international, ces règles se justifiaient par des raisons d'ordre public et que leur application était proportionnée aux risques nouveaux que le média de l'Internet fait courir.

Sans aucun doute, le même raisonnement est applicable à propos des dispositions européennes en matière de Protection des données dans le secteur des communications électroniques. La vie privée est mentionnée expressément par l'article XIV du GATS comme exception possible à la libre circulation des services et les mesures proposées par la directive apparaissent-elles comme strictement proportionnées aux risques nouveaux que le fonctionnement de l'Internet fait encourir à notre vie privée. On ajoute que, sur base de la CEDH, dont la norme est jugée prioritaire par la Cour de Justice européenne vis-à-vis des autres normes internationales, c'est une obligation positive des Etats européens de garantir la vie privée de l'utilisateur d'Internet, cette vie privée considérée comme un droit de l'Homme.

III. Que conclure ?

16. Il est difficile d'éviter plus longtemps la discussion entre les Etats-Unis et l'Europe. Sans doute, cette discussion portera-t-elle sur un meilleur fonctionnement du « *Safe Harbour* » ? Pour moi, il n'est point question de remettre en cause cet acquis ni l'autorégulation, mais simplement d'en approfondir voire de créer les conditions de sa réelle effectivité.

Il s'agira ensemble de réfléchir sur les conditions optimales d'un équilibre entre les besoins de sécurité publique et ceux attachés à la protection d'un droit de l'Homme fondamental pour notre démocratie, entre autres parce que gage de la liberté d'expression.

Il s'agira enfin, de s'accorder sur les règles de base qui protègent l'internaute conçu autant comme consommateur que comme citoyen. Des travaux sont actuellement en cours à propos du SPAM, il faut les élargir.

A cet égard, la ratification toute récente par les Etats-Unis de la Convention du Conseil de l'Europe sur la cybercriminalité le laisse espérer, d'une coopération entière des Etats-Unis et de l'Europe dans la lutte contre les infractions les plus graves en matière de vie privée. A cet égard, l'intrusion dans l'ordinateur d'un internaute n'est-elle pas un « *hacking* » infraction prévue par cette convention et la non interception des communications n'est-elle pas de même garantie par cette Convention.

18. Au-delà, ce qui est en jeu au travers du dialogue US-EU, c'est d'offrir une réponse à l'appel lancé par le récent sommet de Tunis sur la Société de l'Information, en novembre 2005 :

> « *Nous exhortons toutes les parties prenantes à garantir le respect de la vie privée et la protection des informations et données à caractère personnel, et ce par différents moyens : adoption de législations, mise en œuvre de cadres de coopération, élaboration de bonnes pratiques et mise au point de mesures techniques et d'autoréglementation par les entreprises et les utilisateurs. Nous encourageons toutes les parties prenantes, en particulier les Etats, à réaffirmer le droit des personnes à accéder à l'information conformément à la Déclaration de principes de Genève et à d'autres instruments internationaux arrêtés d'un commun accord, ainsi qu'à coordonner leur action au niveau international en tant que de besoin* ».

La dimension globale de l'Internet ne laisse plus de choix à nos pays. Ils doivent s'accorder sur des principes fondamentaux en matière de droits de l'Homme et du droit à la protection des données en particulier. A défaut, nos deux continents remettront en cause l'Unité de l'infrastructure et du réseau en se réfugiant derrière des lois divergentes et en réactualisant des frontières virtuelles en lieu et place des frontières physiques La protection des données est un élément essentiel pour garantir la liberté d'expression et la dignité humaine dans nos sociétés de l'information. Ces valeurs, nos deux continents y sont profondément attachés. Il leur appartient donc ensemble certes par des moyens différents de répondre de manière concrète et effective, à l'appel du Sommet mondial de la Société de l'information.

Ainsi se conçoit la réponse à la question qui guidait mes propos. En matière de protection des droits de l'Homme, il ne peut être question d'impérialisme européen, mais d'un dialogue ouvert où chacun avec sa propre conception des équilibres à trouver entre différentes valeurs (sécurité publique v. libertés individuelles ; intérêt des entreprises v. vie privée) et sa propre tradition réglementaire recherche activement un consensus que le caractère global de l'Internet ne permet plus d'envisager autrement que global. Dans la recherche de ce consensus, l'Europe se doit de continuer à affirmer haut et clair les valeurs de liberté, de dignité et de démocratie qui justifient la protection des données.

Je vous remercie de votre attention.

Yves Poullet

Moxhe, le 24 octobre 2006.