La gouvernance extérieure de l'Union européenne en matière de protection des données à caractère personnel

Valentin Callipel

Lex electronica, vol. 15.3 (printemps/Spring 2011)

Table des matières

Le droit de la protection des données à caractère personnel ne semble pas à première vue concerner directement les relations extérieures de l'Union européenne.

Cependant, dans notre « *société globale de l'information* »[1], caractérisée par les défis qu'impliquent les nouvelles technologies et la mondialisation, les questions relatives à la circulation des informations et notamment à la circulation des données personnelles sont devenues cruciales. Il suffit pour s'en convaincre de se reporter aux succès des entreprises Google ou Facebook, dont l'essentiel des revenus repose sur la collecte et le traitement de ces dernières données précisément. Aussi et puisque « *désormais (…), nulle culture nationale, nulle économie ne sont plus à l'abri de leurs frontières naturelles* »[2] *;* il apparaît que l'Union européenne (UE) ne peut plus définir de façon autonome un standard de protection des données personnelles de ses ressortissants, sans que ce celui-ci ne soit continuellement remis en cause.

En effet, la démultiplication de l'accès aux ordinateurs, à l'Internet, et plus récemment, aux smart phones a multiplié les hypothèses dans lesquelles un individu est devenu à même de semer des informations personnelles, et dans lesquelles des entreprises, dont les activités sont situées en dehors de l'UE, peuvent contourner le niveau de protection garanti aux ressortissants de l'UE.

Aussi, l'UE s'est très tôt saisie de ces questions et s'est efforcée d'engager une large dissémination internationale de son modèle de protection des données dans le but de garantir en toutes circonstances une protection adéquate pour ses ressortissants. Il est donc pertinent de considérer qu'une large facette de la politique européenne en matière de protection des données personnelles appartient en réalité au domaine des relations extérieures de l'Union. L'étude de cette politique constituera le thème d'intérêt principal de cet essai.

---

[1] Yves POULLET, "Comment appliquer les règles de protection des données aux transfert de données personnelles dans une société à la fois globale mais également multi-économique et multiculturelle ?" (2007) 12-1 *Lex Electronica* en ligne : <http://www.lex-electronica.org/docs/articles_33.pdf> (consulté le 23 mars 2011) p.2.

[2] *Id.*

Avant d'envisager précisément l'intérêt de cette thématique, je souhaiterais revenir sur la notion de politique de l'Union européenne à la lumière de l'analyse formulée par Jacques Chevalier dans son ouvrage intitulé « l'État post-moderne »[3].

Selon lui, l'Union européenne est « *une forme d'organisation politique originale, congruente avec l'idée de post-modernité »*[4] car elle ne possède ni les caractéristiques d'un « *authentique État »,* ni un style décisionnel susceptible d'être rattaché à une forme classique de gouvernement. Or, c'est sur ce dernier point que l'analyse de Jacques Chevalier se révèle adéquate pour appréhender la formulation de la politique de l'Union européenne en matière de protection des données personnelles. En effet, en substituant l'acception traditionnelle de « gouvernement » par celle de « gouvernance », Jacques Chevalier restitue la complexité du processus décisionnel de l'Union européenne. Celui-ci est formé autour d'« *un polygone de forces »* dans lequel « *l'Union ne se substitue pas aux États mais ceux-ci interagissent en son sein avec d'autres forces »*[5]. Ainsi, ce processus met en scène « *de multiples acteurs économiques, sociaux, politico-administratifs »*[6] qui agissent sous des formes variées : Directives, Règlements, Accords internationaux, « règles contraignantes d'entreprise »[7], Codes de bonne conduite, clauses contractuelles types, ou encore l'image des entreprises véhiculées par les médias qui sont autant de formes d'action présentes dans la gouvernance européenne des questions relatives à la protection des données à caractère personnel.

Avant d'envisager plus précisément cette gouvernance, il convient de dresser un bref historique de la protection des données en Europe. L'UE a donné naissance à un régime strict et autonome de la protection des données à caractère personnel lesquelles peuvent être définies par l'acception suivante : *« toute information concernant une personne physique identifiée ou identifiable* »[8].

---

[3] Jacques CHEVALIER, *L'Etat post-moderne,* L.G.D.J. 2008.
[4] Préc. note 3 p. 49.
[5] *Id.*
[6] *Id.*
[7] Les règles contraignantes d'entreprise ou encore les « BCR » pour *Binding Corporate Rules* correspondent, d'après la Commission de la protection de la vie privée, a des «*règles qu'une entreprise multinationale peut adopter, qui doivent être obligatoires pour l'ensemble de ses entités, et qui portent sur les transferts internationaux de données personnelles qui sont réalisés au sein du groupe. Pour que les règles d'entreprises contraignantes soient considérées comme offrant des garanties suffisantes quant au respect de la protection des données, il faut qu'elles soient autorisées par les autorités nationales de protection des données compétentes. Une procédure de coopération entre les différentes autorités nationales a été élaborée par le Groupe de travail Article 29* ». Cette définition est accessible sur le site en ligne : <http://www.privacycommission.be> (consulté le 23 mars 2011).
[8] Article 2 *Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel Strasbourg,* 28 janvier 1981, (1981) S.T.E. n° 108.

Originellement conçue comme le corollaire du « *droit au respect de la vie privée* » garanti par la Convention européenne des droits de l'Homme[9], la protection des données s'est progressivement imposée comme une notion autonome justifiant « *l'adoption de mesures concrètes et effectives de protection* »[10]. C'est la convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (Convention 108)[11] qui en détaille la première les contours, avant que son régime ne soit consacré par la directive 95/46/CE (la directive de 95)[12].

Véritable *« pierre angulaire de la législation sur la protection des données dans l'UE »*[13], la directive de 95 visait principalement à la réalisation de deux grands chantiers.

Le premier reposait sur le projet de créer un marché commun capable d'assurer pleinement, en son sein, à la fois la circulation des données personnelles et la protection des personnes qu'elles concernent[14]. Tandis que le second, a consisté à envisager, dès les années quatre-vingt-dix, la question du flux transfrontalier de données à caractère personnel en veillant à ce qu'une protection adéquate soit offerte par les destinataires de flux transfrontaliers[15]. De sorte que ce deuxième aspect devançait le phénomène de mondialisation auquel nous assistons, en envisageant très tôt, l'hypothèse du traitement à l'extérieur de l'Union européenne de ces données.

Par conséquent, la gouvernance européenne en matière de protection des données à caractère personnel a toujours comporté un mécanisme d'adéquation international censé compenser les

---

[9] Article 8 de la *Convention de sauvegarde des droits de l'homme et des libertés fondamentales*, disponible en ligne <http://www.echr.coe.int/NR/rdonlyres/086519A8-B57A-40F4-9E22-3E27564DBE86/0/FRA_Conven.pdf>, (consulté le 23 mars 2011).

[10] Yves POULLET, préc. note 1 p.2.

[11] Préc., note 8.

[12] Directive CE, directive 95/46/CE *du Parlement européen et du Conseil, du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données* (1995) JO, L 281 à la p. 31. (ci-après « la directive de 95 »).

[13] G29, *L'avenir de la protection de la vie privée*, Contribution conjointe à la consultation de la Commission européenne sur le cadre juridique du droit fondamental à la protection des données à caractère personnel Adoptée le 1er décembre 2009, en ligne : <http://www.cnpd.public.lu/fr/publications/groupe-art29/wp168_fr.pdf> (consulté le 23 mars 2011).

[14] Il s'agit du considérant 3 de la directive de 95 préc., note 12 : « *(3) considérant que l'établissement et le fonctionnement du marché intérieur dans lequel, conformément à l'article 7 A du traité, la libre circulation des marchandises, des personnes, des services et des capitaux est assurée, nécessitent non seulement que des données à caractère personnel puissent circuler librement d'un État membre à l'autre, mais également que les droits fondamentaux des personnes soient sauvegardés;* »

[15] Cette question est traitée dans les articles 25 et 26 de la directive de 95 préc., note 12.

disparités de niveaux de protection coexistant dans l'espace globalisé de l'Internet[16]. En effet, il convient de noter qu'en la matière les divergences sont légions. Il suffit de se rapporter au dialogue houleux noué à cet égard entre les USA et l'Europe. « *Under the EU data protection directive, information privacy is a basic human right; the failure of the U.S. legal system to treat it as such offends European values and has led the EU to threaten to suspend information flows to the United States »*[17]. Aussi, il faut voir dans le mécanisme de la directive de 95, comme l'indique la Commission, un outil permettant à l'UE de jouer « *un rôle moteur dans la promotion de normes strictes de protection des données dans le monde entier »*[18]. Bien que la directive de 95 ait de prime abord une portée territoriale (le marché intérieur) et qu'elle ne s'applique pas aux activités telles que la sécurité publique, la défense ou la sûreté de l'État[19], on ne peut cependant minimiser l'impact extraterritorial des dispositions de ses articles 25 et 26.

Ce mécanisme d'adéquation vise à contrôler le transfert de données à caractère personnel vers un pays non membre de l'Union européenne, et de façon plus générale, de l'espace économique européen (CEE)[20]. La combinaison des articles 25 et 26 de la directive conditionne le transfert de données vers un État non membre de l'Union européenne à l'établissement du caractère adéquat de la protection offerte par celui-ci. Plus précisément, en vertu de l'article 25 de la directive, les Etat membres ont l'obligation de légiférer afin

---

[16] A cet égard les exemples sont nombreux, on peut citer ici la distinction substantielle qui caractérise les conceptions américaine et européenne à propos de la vie privée. Quand les premiers rattachent ce concept à la notion de liberté, les seconds se réfèrent quant à eux à la notion de dignité qui a pour conséquence de faire peser sur l'Union européenne une obligation positive visant à garantir une protection adéquate à ses ressortissants en toute circonstance. La position américaine renvoie davantage à l'autodétermination, et préconise en la matière un mécanisme d'autorégulation.

[17] Fred H. CATE, "The Changing Face of Privacy Protection in the European Union and the United States" (1999) 33-173 *Indiana Law Rev*, en ligne<http://ssrn.com/paper=933090> *abstract* (consulté le 23 mars 2011).

[18] COMMISSION EUROPEENNE *Une approche globale de la protection des données à caractère personnel dans l'Union européenne,* 4 novembre 2010, disponible en ligne <http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_fr.pdf> (consulté le 23 mars 2011). Cette communication s'inscrit dans le cadre d'une proposition législative pour 2011 tendant à réviser la directive de 1995 relative à la protection des données.

[19] Il s'agit du considérant 13 de la directive de 95 *op.cit.* note 12 *« (13) considérant que les activités visées aux titres V et VI du traité sur l'Union européenne concernant la sécurité publique, la défense, la sûreté de l'État ou les activités de l'État dans le domaine pénal ne relèvent pas du champ d'application du droit communautaire, sans préjudice des obligations incombant aux États membres au titre de l'article 56 paragraphe 2 et des articles 57 et 100 A du traité; que le traitement de données à caractère personnel qui est nécessaire à la sauvegarde du bien-être économique de l'État ne relève pas de la présente directive lorsque ce traitement est lié à des questions de sûreté de l'État; »*

[20] La CEE est constituée de la Communauté européenne et trois membres de l'association européenne de libre-échange (AELE) : l'Islande, la Norvège et le Liechtenstein. Se reporter aux explications données à ce sujet sur le site : http://www.privacycommission.be.

d'interdire le transfert de données en direction de pays non membres qui n'offriraient pas un niveau de protection adéquat.

Ainsi l'adéquation se pose comme un concept fort participant d'une dissémination internationale du modèle de protection adopté par l'UE. L'évaluation du caractère adéquat peut faire l'objet d'une appréciation souveraine de l'Union, par le biais d'une procédure dite « d'homologation »[21] ou être conditionnée au respect des « *Safe Harbour principles* »[22] pour les entreprises américaines, ou bien encore résulter de l'intégration de stipulations contractuelles types[23].

En dépit des nombreux instruments mis en place pour y parvenir, cette politique d'adéquation paraît continuellement remise en cause au gré des avancées technologiques qui se posent comme autant de nouveaux défis toujours plus difficiles à relever (voir par exemple les développements du Cloud computing et de la sous-traitance) mais peine également à former un consensus au plan international, en raison de divergences culturelles ou économiques (en témoignent les négociations houleuses avec les États-Unis à propos des accords SWIFT[24] ou PNR[25]).

Cependant, la récente consécration, depuis le Traité de Lisbonne, de la protection des données « *comme un droit autonome par rapport à celui de la vie privée* » par la Charte des droits fondamentaux de l'Union européenne [26], ainsi que la suppression des piliers communautaires[27], semblent avoir réactualisé le *leadership* de la gouvernance européenne sur

[21] Voir *infra.* p. 8 et suivantes.
[22] Voir *infra.* p. 13 et suivantes.
[23] Voir *infra.* p. 16 et suivantes.

[24] Le programme de surveillance du financement du terrorisme aussi appelé TFTP, fait l'objet d'un développement approfondi dans la première partie.
[25] *L'accord Passenger Name Record (PNR)* fait l'objet d'un développement approfondi dans la seconde partie.
[26] Yves POULLET préc., note 1 p. 3 évoquant les articles 7 et 8 de la *Charte des droits fondamentaux de l'union européenne* disponible en ligne : <http://www.europarl.europa.eu/charter/pdf/text_fr.pdf> (consulté le 23 mars 2011), laquelle a acquis depuis le 12 décembre 2007 une force juridique contraignante avec le Traité de Lisbonne
[27] Voir notamment les développements suivants : *« The structure of the European Union, as outlined by the Maastricht Treaty, is based on three pillars: 1. the Community pillar, corresponding to the European Communities (first pillar); 2. The common foreign and security policy (CFSP), provided for by Title V of the EU Treaty (second pillar); 3. police and judicial cooperation in criminal matters, provided by Title VI of the EU Treaty (third pillar). Directive 95/46 is not to be applied to the processing of personal data in the course of activities falling under the second and third pillars »* in M. NINO "The Protection of Personal Data in the Fight Against Terrorism: New Perspectives of Pnr European Union Instruments in the Light of the Treaty of Lisbon." (2010). 6-1 *Utrecht Law Review,* p.69.

cette question. L'année 2011 devrait notamment donner lieu à une réforme législative d'envergure, visant à revoir la « *stratégie de l'Union européenne pour la protection des données personnelles* »[28].

Entre quête de convergence et tentation unilatéraliste, il semble intéressant de tenter d'identifier la voix exprimée par l'Union européenne à l'échelle internationale sur ces questions. Quelle est cette politique d'adéquation ? Quelle est sa légitimité ? Quels en sont les instruments ? Et finalement, quelle est son efficacité ? Voici, les questions auxquelles j'essayerai de répondre dans les lignes qui suivent.

Après avoir tenté de décrire les modalités de l'extension de la sphère de sécurité de l'Union européenne se rapportant à la circulation des données personnelles de ses ressortissants dans le cadre du marché intérieur (I), je tenterais de relativiser l'effectivité du modèle ainsi véhiculé (II).

[28] Préc., note 18.

I / La quête de l'unisson européen : gage d'une dissémination de son modèle de protection des données personnelles :

Attachée à promouvoir l'élaboration de normes juridiques et techniques élevées en matière de protection des données au niveau international, l'UE n'en oublie pas pour autant les besoins et les avantages qui découlent du commerce international. Aussi, la gestion de l'impact extraterritorial des dispositions des articles 25 et 26 de la directive paraît empreinte d'un certain pragmatisme. Si la détermination du caractère adéquat de la protection offerte par l'Etat tiers sous la forme de « l'homologation » semble rigoureuse (A) des hypothèses plus souples sont envisagées lorsque des réajustements apparaissent nécessaires (B).

A/ Le réajustement démocratique de la politique d'adéquation par homologation de l'Union européenne :

1/ Le cadre de la politique d'adéquation par homologation :

Comme le note Yves Poullet, « *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 de protection offert par le destinataire »*[29] laquelle pourrait être synonyme d'une forme d'impérialisme.

La recherche d'une adéquation se veut donc en apparence exclusive d'une approche unilatéraliste (qui consisterait en une simple transposition des principes contenus dans la directive de 95 dans les législations des Etats tiers). Cette précaution illustre la diversité des conceptions qui existent à l'échelle internationale à propos des notions de vie privée et de données personnelles. Parfois antagonistes, les approches retenues par les différents partenaires de l'UE sont généralement le fruit de divergences culturelles qui en apparence ne peuvent être dissoutes dans une simple transposition législative. Il suffit par exemple

[29] Yves POULLET Préc., note 1, p. 3

d'envisager le profond clivage qui sépare les conceptions américaine et européenne à ce sujet. En effet, selon Adam Todd, « *the different approaches to data privacy result from very different perspectives of the United States and the European Union on privacy in general. The European perspective on privacy focuses on dignity, while the American perspective is more focused on liberty »*[30].

Si l'approche retenue par l'UE se veut *a priori* dépourvue d'unilatéralisme, elle ne renonce pas, pour autant, aux exigences de protection des données qui ont cours au sein de ses frontières et par conséquent refuse en principe le transfert de données en direction de pays qui ne présenteraient pas une protection adéquates de celles-ci[31]. Ainsi, en application de l'article 25 (6) de la directive[32], la Commission peut prendre « *une décision d'adéquation du droit étranger »*[33] afin d'autoriser des flux de transfert de données avec ce dernier. Cette homologation est donnée à l'issue d'une analyse comparée des deux législations, qui suppose d'évaluer le contenu de la protection offerte ainsi que les moyens mis en place pour s'assurer du respect de ce contenu par l'Etat destinataire du flux de données. Originellement la décision d'adéquation était rendue par la Commission après avis consultatif du groupe de l'article 29 (G29)[34]. Or, comme l'évoque Thomas-Sertillanges, cet avis est d'autant plus favorable « *que le texte étranger s'inspirera de la directive, comme c'est d'ailleurs souvent le cas ».* À ce jour sept pays on fait l'objet d'une décision d'adéquation et quatre ont reçu un avis favorable du G29 (l'Argentine, le Canada, la Suisse, Jersey, Guernesey, l'Ile de Man et depuis le 31 janvier dernier l'Israel)[35]. Une fois que la Commission a rendu une décision favorable il s'opère, en quelque sorte, une extension de la sphère de sécurité de l'Union, et dès lors, un responsable de traitement basé au sein de celle-ci pourra valablement exporter des données personnelles

---

[30] Adam. G. TODD, "Painting a Moving Train: Adding "Postmodern" to the Taxonomy of Law "(2008) 40 *The University of Toledo Law Review* 105, p 136, citant James Q. WHITMAN, "The Two Western Cultures of Privacy : Dignity versus Liberty", (2004), 113 *Yale Law Journal.* 1151.

[31] Ces critères mériteraient de faire l'objet d'une analyse à part entière, on peut toutefois en citer les plus importants : notamment, légitimité, compatibilité de la communication des données à un tiers avec le traitement d'origine, information des personnes concernées.

[32] Directive de 95, préc. note 12.

[33] Jean-Baptiste THOMAS-SERTILLANGES, "Libre circulation des données à caractère personnel et protection de la vie privée, entre marché intérieur et ELSJ", (2011), 24 *Les petites affiches* 3, p.6.

[34] La Directive de 1995 a mis en place un organe consultatif indépendant communément appelé groupe de travail « Article 29 » (le G29) où se retrouvent les représentants des organes de contrôle des États membres concernant les questions de protection des personnes à l'égard du traitement des données à caractère personnel. À la demande de la Commission européenne, le G29 émet des avis relatifs au « niveau de protection dans la Communauté européenne et dans les pays tiers ».

[35] Décision CE, *Décision 2011/61/CE de la Commission du 31 janvier 2011 constatant, conformément à la directive 95/46/CE du Parlement européen et du Conseil, le niveau de protection adéquat des données à caractère personnel assuré par l'État d'Israël concernant le traitement automatisé des données à caractère personnel,* (2011) JO L 281 à la p. 31.

vers l'un de ces pays destinataires (à condition bien sûr de respecter les autres obligations de la directive de 95)[36].

2 / Les acteurs de cette politique d'adéquation par homologation :

La gouvernance menée par l'Union, et dont la Commission se veut ici la représentante, s'est traduite par une large dissémination de son modèle de protection des données. Cependant le modèle ainsi véhiculé a pu faire l'objet de certaines critiques qui tiennent à la procédure d'adéquation utilisée mais également au modèle de protection des données lui-même.

S'agissant de la procédure d'homologation, on a pu reprocher à la Commission d'opérer un contrôle stricte des contenus des législations plutôt que de leur effectivité. Plus généralement, cette faculté d'homologation a pu sembler pour les citoyens de l'UE et leurs représentants, les membres du Parlement européen, comme l'exercice d'une prérogative fortement discretionnaire.

S'agissant du modèle même de protection des données personnelles, il faut prendre conscience de l'effet relatif des mécanismes d'harmonisation, tels qu'ils existent au sein de l'Union européenne et tels qu'ils découlent de la directive de 1995. Il serait en effet optimiste de considérer qu'aujourd'hui le modèle véhiculé à partir de l'Union européenne est une architecture homogène (voir notamment les projets visant à instaurer un cadre global unique[37]). Aussi, il apparaît encore nécessaire d'engager une harmonisation intraeuropéenne accrue « *sans laquelle l'impression de conglomérat disparate persisterait avec des pratiques très hétérogènes au niveau des vingt-sept Etats »*[38]. En témoigne notamment, l'« *application divergente des règles de l'UE par les autorités de protection des données* »[39]. La protection des données demeure un débat sociétal de grande ampleur qui cristallise la diversité des cultures et des traditions qui se jouent en Europe.

---

[36] Op.cit préc. note 31

[37] La recherche d'un cadre global de protection des données à caractère personnel fait l'objet d'une étude qui a été rendu publique dans une communication de la Commission européenne préc., note 18.

[38] Analyse de la communication de la Commission préc., 18, en ligne : < http://eulogos.blogactiv.eu> (consulté le 22 mars 2011).

[39] Préc., note 18 p.20.

Dès lors, la question de l'homologation des flux transationaux de données a pu faire l'objet de vives polémiques, et révèler la variété des forces intervenant dans le processus décisionnel de la gouvernance européenne.

Les affaires PNR[40] et SWIFT[41], qui sont les principaux accords de l'entente transatlantique en matière de lutte contre le terrosime, présentent les enjeux possibles de la collecte de données personnelles.

C'est à l'issue de vives réactions de la société civile ainsi que du Parlement européen que le processus d'homologation a été modifié et a fait l'objet d'un réajustement que l'on pourrait qualifier de « démocratique ».

3/ Le réajustement démocratique de cette politique d'adéquation par homologation :

Avant l'entrée en vigueur du traité de Lisbonne, le Conseil et le Parlement avaient délégué à la Commission le pouvoir de décider si un pays tiers offrait un niveau de protection adéquat des données à caractère personnel.

L'abandon de cette prérogative est finalement assez paradoxal compte tenu de l'intérêt grandissant dont à fait preuve par la suite le Parlement européen à propos de ces questions.

En effet, le Parlement a exprimé, à plusieurs reprises ses préoccupations, par voie de résolution, à propos de la protection des données, du fichage ethno-racial de *« la possible introduction de scanners corporels en vue de renforcer la sécurité aérienne, les données biométriques dans les passeports et les instructions consulaires communes, la gestion des frontières, l'internet et l'extraction des données »*[42] et a acquis depuis, une certaine crédibilité qui a pu êtres concrétisée grâce au Traité de Lisbonne.

---

[40] Il s'agit du transfert des données à caractère personnel contenues dans les dossiers des passagers aériens transférés au Bureau des douanes et de la protection des frontières des Etats-Unis. Cet accord fait l'objet d'une étude approfondie dans la seconde partie de cet essai.

[41] Il s'agit du programme de surveillance du financement du terrorisme aussi appelé TFTP.

[42] Alessandro DAVOLI, "Protection des données à caractère personnel", (2010) en ligne : < http://www.europarl.europa.eu/ftu/pdf/fr//FTU_4.12.8.pdf> (consulté le 22 mars 2011).

En effet, depuis l'entrée en vigueur du traité de Lisbonne la procédure, dite « d'approbation », a été étendue aux accords internationaux ayant trait au domaine de la protection des données et du partage d'informations[43].

Cette consécration vient confirmer la montée en puissance de l'influence du Parlement européen sur ces questions. Aussi, celle-ci, s'est notamment traduite, à ce jour, par le refus de ratifier huit des accords conclus selon l'ancienne procédure[44]. Le Parlement européen a notamment utilisé ses pouvoirs en février 2010 en rejetant l'application provisoire de l'accord sur le programme de surveillance du financement du terrorisme (TFTP) (anciennement connu comme accord SWIFT, en raison du réseau SWIFT utilisé pendant plusieurs années par le Trésor des États-Unis pour identifier, localiser et surveiller les personnes soupçonnées d'activités terroristes). Comme le note la Commission dans une récente communication : « *À la suite de la résolution du Parlement du 8 juillet 2010, l'accord TFTP est entré en vigueur en août 2010. L'accord final répond aux préoccupations majeures du Parlement sur plusieurs aspects importants, tels que l'élimination massive du transfert des données, l'interdiction de l'extraction des données, la possibilité de créer un mécanisme européen de TFTP, un nouveau rôle pour Europol, la nomination d'un superviseur européen indépendant et les droits de recours pour les citoyens européens* »[45].

Fort de ces nouvelles compétences le Parlement jouit d'une nouvelle crédibilité et pèse davantage dans le processus décisionnel. De sorte qu'il n'est pas étonnant que la Commission ait récemment envisagé « *de clarifier la procédure d'évaluation du caractère adéquat du niveau de protection assuré dans un pays tiers ou une organisation internationale et de préciser les critères et conditions applicables »*[46].

Cette brève analyse de la politique d'adéquation entreprise par l'UE tant au plan interne qu'externe est révélatrice de cette quête d'unisson en matière de protection des données

[43] Le Parlement européen examine un projet d'acte transmis par le Conseil ; il statue sur son approbation (sans la possibilité de l'amender) à la majorité absolue des voix exprimées.
[44] C'est le cas, notamment, pour l'accord *SWIFT* conclu entre les Etats-Unis et l'Union qui a été signé par le Conseil le 30 novembre 2009. L'accord intermédiaire, entré en vigueur le 1er février 2010, a été rejeté par la Commission des libertés civiles. En adoptant le rapport de Jeanine Hennis-Plasschaert (ADLE, NL), la Commission LIBE a, en effet, marqué son désaccord avec SWIFT et invité la Commission et le Conseil à initier des travaux pour aboutir à un autre accord à long terme avec les Etats-Unis. Décision qui a été suivie, lors de la plénière du 11 février 2010, par l'ensemble du parlement européen qui a rejeté l'accord SWIFT par 378 votes pour, 196 contre et 31 abstentions.
[45] Préc., note 42.
[46] COMMISSION EUROPEENNE prèc., 18, p.18.

personnelles. Si en apparence, cette politique s'affiche comme une recherche stricte d'adéquation entre les ordres juridiques, on observe que cette dynamique et également accompagnée d'un mouvement plus souple que l'on pourrait qualifier de plus pragmatique.

B/ Le recours à d'autres instruments de régulation censés accorder les tiers à la politique de l'Union européenne :

Dans certaines hypothèses l'adéquation par homologation s'avère impossible. En effet, parfois les ordres juridiques tiers ne prévoient tout simplement aucune protection des données personnelles, ou présentent des divergences d'approches trop fortes pour qu'il soit procédé à une simple adéquation par homologation de la législation du partenaire étatique.

Ayant à cœur de réguler la protection des données, l'Union européenne emprunte par conséquent d'autres voies, sous la forme d'instruments internationaux *Sui generis* qui s'apparentent à des formes autonomes de contractualisation. Concluant tantôt des accords avec des partenaires Étatiques, tels que les États-Unis (grâce aux *Safe Harbour Principles*) (**1**), l'UE ne néglige pas pour autant les acteurs privés (entreprises multinationales) et propose des formes d'adéquation d'un nouveau genre (« *dans le cadre d'un contrat ou de règles internes à l'entreprise »*[47]) qui représentent à bien des égards un laboratoire de ce que pourraient être d'autres modalités de gouvernance de ses relations extérieures (**2**).

1/ Vis-à-vis des États tiers : L'exemple du « Safe Harbour Act » :

Alors que la protection des données au sein de l'Union européenne est prévue par un instrument à vocation globale tel que la directive de 95, on constate en revanche qu'aux Etats-Unis, cette protection fait l'objet d'un traitement sectoriel, fragmenté, ne présentant pas de cohérence globale. Seuls certains domaines sont couverts, comme la protection des données médicales par le « *Health Insurance Portability and Accountability Act »* (HIPAA), de sorte

[47] UNESCO, *Le droit fondamental des personnes à la protection des données personnelles: les défis à relever sur le plan national, régional et mondial,* discours prononcé par Marie Georges, Conseiller pour la prospective et pour le développement du président de la Commission nationale de l'informatique et des libertés (CNIL), (Paris 2007) en ligne : < http://portal.unesco.org/ci/en/files/26953/12121570985Georges-Marie.pdf/Georges-Marie.pdf> (consulté le 23 mars 2011).

que « *outside of these discrete areas, much of U.S. data protection is subject to self regulation. Online data collection, in particular, remains unregulated, affording little privacy to users* »[48].

De lors l'interdiction de transférer des données personnelles à destination de pays ne présentant pas un niveau de protection adéquat prévue par la directive de 95 a eu pour effet de pénaliser les entreprises américaines. Ainsi, *« to shield U.S. companies from penalities under the E.U. Directive, the United States and the European Union entered into the Safe Harbour Agreement which intented to bridge their different approaches »*[49].

Le mécanisme des *Safe Harbour,* est une réponse négociée entre les Etats-Unis[50] et l'Union européenne [51] à la directive de 95. Il s'agit d'un compromis, censé réunir les divergences présentes dans ces deux ordres juridiques. Il est optionnel et permet aux entreprises et organisations[52] américaines d'adhérer, sur la base du volontariat, aux principes du *Safe Harbour*[53]. Ces principes sont publiés par le Département américain du commerce et ont été reconnus comme garantissant un niveau de protection adéquat au regard de la directive par la Commission européenne en juillet 2000[54].

Ce mécanisme est doté d'une portée contraignante atypique, qui présente davantage les caractéristiques d' *« une forme d'auto certification sur une base déclarative »*[55] car il n'est pas prévu de contrôle préalable. Cependant la plupart des sociétés américaines ont recours à un tiers certificateur, à l'image de la société Trust-e. Si en apparence le mécanisme paraît exempt de force contraignante, il convient tout de même de préciser que « *les sociétés américaines peuvent être sanctionnées en raison d'une déclaration mensongère, sur la base du False Statement Act, 18 US C § 1001* »[56]. Il s'agit donc d'une forme d'autorégulation

---

[48] Adam TODD préc., note 30 p. 135
[49] Adam TODD préc., note 30 p. 135-136.
[50] Représentés par le Département américain du commerce et l'Agence nationale de l'information
[51] Représentée par la direction générale « Marché intérieur » de la Commission européenne.
[52] La liste des entreprises et organisations ayant adhérées aux principes de la « sphère de sécurité » est disponible à l'adresse suivante : http://web.ita.doc.gov/safeharbor/shlist.nsf/webPages/safe+harbor+list.
[53] Ces principes sont notamment décrits en ligne : <www.export.gov> (consulté le 23 mars 2011).
[54] Décision CE, *Décision* 2000/520/CE de la Commission du 26 juillet 2000 faisant suite à la Directive 95/46/CE du Parlement européen et du Conseil *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 États-Unis d'Amérique* JO, L215 à la p7.
[55] Elisabeth QUILLATRE, « La libre circulation des données à caractère personnel au sein du marché intérieur et de l'ELSJ et nouveaux outils de régulation », (2011), 24 *Les petites affiches* 10, p.11.
[56] *Id.*

reposant sur le modèle véhiculé par l'Union qui en dépit de son caractère facultatif reste incitatif pour les entreprises voulant commercer avec les Etats-membres de l'Union européenne.

Recouvrant plusieurs qualificatifs juridiques « *mécanisme d'auto-certification sur un modèle administratif, cadre juridique supplétif ou optionnel, engagement unilatéral* »[57], le Safe Harbour Agreement demeure un instrument « *ayant vocation à organiser la coordination internationale des droits nationaux ou régionaux de la protection de données* »[58]. Il constitue donc compte tenu de l'éloignement entre les imaginaires juridiques américain et européen sur ces questions, une solution permettant d'envisager une protection des ressortissants communautaires dans l'hypothèse où leurs données personnelles seraient traitées sur le territoire américain.

S'il ne faut pas surévaluer l'engouement de l'adhésion des entreprises américaines à ces principes, on peut tout de même noter qu'en 2007 plus de 1000 d'entre elles avaient procédé à cette certification[59]. On compte d'ailleurs parmi elles les plus concernées par les données personnelles dont Facebook et Google qui ont également eu recours à l'organisme de certification Trust-e[60].

Comme nous le verrons dans une seconde partie, le mécanisme de régulation sur le lequel repose le Safe Harbour, n'est pas exempt de critiques. Il conserve cependant le mérite d'envisager une nouvelle forme de gouvernance ambitieuse des questions ayant trait à la protection des données personnelles dans le cadre des échanges internationaux. De part la variété des acteurs qui y participent, des États (USA), un ensemble régional (l'Union européenne) et certaines de ses institutions, des entreprises ainsi que des tiers certificateurs, il se pose comme une forme de gouvernance autonome susceptible de poser les bases d'autres formes de coopération de l'Union européenne avec ses partenaires internationaux.

---

[57] *Id.*
[58] Elisabeth QUILLATRE préc., note 55.
[59] Voir Vinita BALI, "Data Privacy, Data Piracy: Can India Provide Adequate Protection for Electronically Transferred Data?" (2006). bepress Legal Series. Working Paper 1594 en ligne : http://law.bepress.com/expresso/eps/1594 (consulté le 23 mars 2011).
[60] Voir le site en ligne : <https://safeharbor.export.gov> (consulté le 23 mars 2011).

Si le pont entre les Etats-Unis et l'Union européenne a pu être construit sous la forme des *Safe Harbor Principles*, il est des hypothèses où la faiblesse de la protection des données personnelles offertes dans les Etats tiers ne permettait ni de mettre en œuvre le mécanisme d'adéquation par homologation, vu plus haut, ni non plus de recourir au dernier mécanisme envisagé. Dans ces circonstances, l'Union européenne s'est attelée a promouvoir de nouvelles formes de régulation reposant sur un modèle de contractualisation d'un nouveau genre : les clauses contractuelles types de la commission ou les « règles contraignantes d'entreprise »[61].

2/ Vis-à-vis des acteurs privés : le recours à la contractualisation

Inspirée par les travaux de Jürgen Habermas[62], la contractualisation est devenue une forme courante de l'action publique. Aussi, il est intéressant d'envisager l'utilisation qui en faite par l'Union européenne dans l'hypothèse où un État tiers ne présente pas de protection adéquate au sens de la directive de 95 (a) ou bien lorsqu'une société multinationale désire réaliser des flux intra-groupe et dont certains membres sont établis en dehors de l'Espace économique européen (b).

a) Les clauses contractuelles types :

Les articles 26(2), 26(3) et 26(4), de la directive de 95 prévoient qu'un État membre peut autoriser un transfert de données à caractère personnel vers un État tiers lorsque le responsable du traitement[63] offre « *des garanties suffisantes au regard de la protection de la vie privée et des libertés et des droits fondamentaux des personnes* »[64]. La protection est ainsi assurée au moyen d'un contrat liant celui qui envoie les données et celui qui les reçoit et contenant des garanties suffisantes au regard de la protection des données. Ces clauses contractuelles types font l'objet d'un contrôle par les autorités compétentes des Etats-membres (par exemple la CNIL en France). Afin de faciliter la tâche des responsables de traitement dans la mise en œuvre de contrats de transfert, la Commission européenne met à

[61] Préc., note 7.
[62] Ces thèses sont notamment mis en valeur dans l'ouvrage suivant : Jurgen HABERMAS, *Droit et Démocratie — Entre faits et normes*, traduit de l'anglais par R. Rochlitz et C. Bouchindhomme, Paris, Gallimard, 1997.
[63] Un responsable de traitement est « *la personne, l'autorité publique, le service ou l'organisme qui détermine ses finalités et les moyens du traitement* », voir site de la CNIL en ligne : www.cnil.fr (consulté le 23 mars 2011).
[64] Article 26 (2) de la directive de 95 préc., note 12.

leur disposition des modèles de contrats-type qui sont automatiquement considérés comme offrant des garanties suffisantes. Ces clauses contractuelles types résultent de décisions de la Commission et concernent d'une part, les transferts de responsables de traitement à sous-traitants[65] et d'autre part les transferts de responsables de traitement à responsables de traitement[66]. Dès lors qu'un responsable de traitement mettra en œuvre un transfert régi par les stipulations de ces clauses contractuelles type, ce dernier bénéficiera d'une présomption de protection adéquate.

Grâce à cet instrument, comme le suggère Thomas-Sertillanges, de nombreuses entreprises « *établies hors de l'Union européenne ont finalement adhérée ponctuellement et indirectement au régime de la directive. En se soumettant volontairement à ce cadre, elles viennent se greffer temporairement à la sphère de sécurité du marché intérieur et bénéficient par conséquent du principe de libre circulation des données, comme si elles étaient établies sur le territoire de l'Union européenne* »[67].

Cette allocation de garanties suffisantes par la voie contractuelle présente la particularité *« d'incorporer et de se substituer à des obligations d'origine légales* »[68]. Ce mécanisme propose une forme nouvelle de régulation empreinte d'un principe de réalité. Il s'agit en effet d'associer, non plus simplement des partenaires étatiques[69], mais également des acteurs privés à la diffusion du modèle de protection des données que s'est choisie l'Union européenne. Contrats d'un nouveau genre, puisqu'ils participent d'une contractualisation de la directive de 95, on voit là un moyen de palier à l'inertie et à la lourdeur que peuvent présenter les processus normatifs interétatiques traditionnels.

Si ce mécanisme répond en partie au besoin de transferts ponctuels de données, l'Union européenne s'est également attachée à intégrer dans sa gouvernance un encadrement plus systématique de ces transferts de données pour les besoins notamment des multinationales.

---

[65] Décision CE, *Décision 2002/16/CE de la Commission du 27 décembre 2001 relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des sous-traitants établis dans des pays tiers en vertu de la directive de 95/46* (2002), JO L 281 du 23.11.1995, p. 31.

[66] Décisions CE, *Décision 2001/497/CE de la Commission du 15 juin 2001 relative aux Clauses contractuelles types pour le transfert de données à caractère personnel vers des pays tiers en vertu de la directive 95/46/CE* (2001), JO L181 à la p. 19.

[67] Jean-Bapstiste THOMAS-SERTILLANGES préc., note 33 p.7.

[68] *Id.*

[69] En effet, *in fine,* ce que négocient les Etats-Unis bénéficient à ses entreprises et organisations.

b) Les règles internes d'entreprises multinationales :

Afin d'éviter à une entreprise multinationale, dont certains membres sont établis en dehors de l'Espace économique européen, d'avoir à conclure un contrat à chaque fois qu'elle désire réaliser des flux de donnée personnelles intra-groupe, il a été mis en place des règles d'entreprises contraignantes les « Binding Corporate Rules » (ci-après BCR) qui sont une forme de code de bonne conduite.

Comme on peut le lire sur le site de la Commission, les BCR : « *are used by multinational companies in order to adduce adequate safeguards for the protection of the privacy and fundamental rights and freedoms of individuals within the meaning of article 26 (2) of the Directive 95/46/CE for all transfers of personal data protected under a European law. To that extent, BCR ensure that all transfers are made within a group benefit from an adequate level of protection »*[70].

L'homologation des BRC se fait auprès des autorités de protection des données personnelles de chacun des États membres selon des critères qui ont été déterminés par le groupe de l'article 29 (G29)[71]. C'est ainsi qu'une entreprise comme e-Bay s'est conformée à cette procédure auprès de l'autorité luxembourgeoise compétente en novembre 2009.

Comme l'envisagent certains auteurs, la procédure européenne de BCR, en ciblant les multinationales, servirait de substrat à : « *l'universalisation des principes de protection des données personnelles »* [72]. Si on peut voir là, un outil d'une rare efficacité, il est également le révélateur de l'harmonisation relative qui règne en matière protection des données personnelles au sein de l'Union. En effet, pour obtenir l'homologation de ces BCR une entreprise devra obtenir l'accord des vingt-sept autorités de protection des données personnelles. Cette procédure se révèle être très fastidieuse. Il faut prévoir des mois voire des années pour la valider, ce qui explique sans doute qu'à ce jour seules dix entreprises

[70] En ligne : <http://ec.europa.eu/justice/policies/privacy/binding_rules/index_en.htm> (consulté le 23 mars 2011).
[71] Le groupe de l'article 29 a adopté un document de travail sur ces questions, dit document WP 74 en ligne : http://www.privacycommission.be/fr/static/pdf/flux-transfrontieres/wp74.pdf (consulté le 23 mars 2011).
[72] Préc., note 33.

multinationales y ont eu recours. Notons toutefois que depuis « *le 1er octobre 2008, dix-huit autorités nationales se sont entendues pour que le projet d'une société, une fois validé par l'autorité de protection du pays d'origine, puisse bénéficier d'une présomption de conformité dans l'ensemble du territoire européen »*[73].

Menées depuis et à partir de l'Union européenne, ces politiques d'adéquation empruntent des formes de dissémination de son modèle de protection des données plus ou moins strictes. Largement caractérisée par un principe de réalité, cette gouvernance européenne révèle la diversité des acteurs qui participent au processus décisionnel en la matière. La composition de ce *polygone de force,* auquel nous faisions référence dans l'introduction, met en scène à la fois des multinationales, divers acteurs de la société civile, le Parlement européen ainsi que par exemple le Département du commerce des Etats-Unis. Ces formes d'actions ont le mérite de reconnaître l'importance de ces différents acteurs et de les resituer dans des rapports de droit. Cependant aussi ambitieuse et illustrative de ce que pourraient être les politiques extérieures de l'Union européenne dans d'autres domaines, cette gouvernance européenne, compte tenu des spécificités du médium sur lequel repose le transfert des données personnels, pêche par son effectivité pratique. En effet, sans une perspective globale, capable de dépasser une vision positiviste traditionnelle, les efforts entrepris par l'Union européen en la matière tiendraient davantage, comme nous allons le voir, à un coup d'épée dans l'eau.

[73] Jean-Bapstiste THOMAS-SERTILLANGES préc., note 33 p.9.

II / La politique d'adéquation internationale ou les jalons d'un dialogue entre l'Union européenne et ses partenaires :

Depuis l'entrée en vigueur de la directive de 1995, l'Union européenne est présentée comme la pionnière de la promotion du droit fondamental à la protection des données à l'échelle internationale. De nombreux États ont suivi cette voie dans le sillon de la législation européenne. Doit-on parler de mimétisme ? *A priori,* il serait plus juste d'évoquer simplement l'influence de l'Union européenne. Comme le fait observer en 1997, Colin Bennett « *Nowhere has the Data Protection Directive been the sole reason for another country's passing a data-protection law. On the other hand, it has certainly been one important influence* »[74]. Aussi, plutôt que d'évaluer le coefficient de perforation de la législation européenne à l'échelle planétaire, il semble davantage pertinent d'envisager son application pratique à l'heure de l'Internet. En effet, la protection des données est un droit « *intimately connected to high technology and the computer age »[75],* qui embrasse par conséquent les contingences de ces médiums, à savoir : « *uncertainty, complexity and indetermination »[76]*. Si la gouvernance européenne s'avère proactive, elle reste tout de même confrontée à une certaine ineffectivité pratique, qui tient à la fois aux difficultés de réguler un medium qui repose sur une technologie mouvante, mais également paradoxalement à la difficulté de cristalliser un consensus à l'intérieur comme à l'extérieure de ses frontières sur ces questions (A). Compte tenu de ces défis, l'année 2011 devrait donner lieu à une réforme législative européenne d'envergure visant à revoir la « *stratégie de l'Union européenne pour la protection des données personnelles »[77]*. Aussi salutaire que puisse être le dynamisme européen, il semble toutefois qu'au delà de la recherche d'une solution unilatérale, la bonne gouvernance des questions relatives à la protection des données ne doive être recherchée dans un dialogue afin d'élaborer une solution partagée avec l'ensemble des partenaires de l'Union,

---

[74]Colin J. BENNETT, *"*Convergence Revisited: Toward a Global Policy for the Protection of Personal Data*",* dans Philip E. AGRE et Marc ROTENBERG *Technology and privacy* Cambridge, The New Landscape. Cambridge, MA: MIT Pres, 1997, p. 99, à la page 110.

[75] Adam TODD préc., note 48 p. 140

[76] Pierre TRUDEL, "The Development of Canadian Law with respect to E- government", dans J. E. J. PRINS *Designing e-Government*, Utrecht, the International Academy of Comparative Law Congress (2006), pages 113-164, à la page 113.

[77] COMMISSION EUROPEENNE, préc., note 18.

tant étatiques que privés (B).

A/ Le déficit de l'unilatéralisme : l'Union européenne condamnée au dialogue ?

Si la gouvernance européenne des questions relatives à la protection des données personnelles est innovante et dynamique, il reste qu'elle demeure, au prix de larges investissements de temps et d'argent, bien souvent ineffective (1) et continue de cristalliser des approches divergentes à l'extérieur comme au sein de l'Union européenne. (2).

1/ Le manque d'effectivité inhérent aux mécanismes d'adéquation utilisés :

Alors qu'est envisagée la refonte des mécanismes introduits par la directive de 95, il convient d'envisager le bilan de la gouvernance entreprise jusqu'à présent, lequel peut être qualifié de contrasté.

En effet, comme le fait remarquer un peu abruptement, Omer Tene : « *Enforcement is a sore issue for the EU DPD* (EU Data Protection Directive). *It is an open secret that the framework is largely not enforced »*[78]. Il convient à cet égard de relayer certaines des critiques qui lui sont faites et qui tiennent d'une part, au fait qu'il s'agit d'un mécanisme lourd et complexe à mettre en œuvre et d'autre part à l'existence de nombreuses voies de contournements.

Telle qu'envisagée par la directive de 95, la politique d'adéquation par homologation[79] se heurte en pratique à la difficulté d'engager un contrôle effectif des législations comparées. A cet égard, il convient de noter le caractère quelque peu illusoire de cette tâche. En effet, lister et engager une procédure de contrôle de l'adéquation des ordres juridiques offrant un niveau de sécurité adéquat consiste en définitive à déterminer une liste blanche. On sait que l'élaboration d'une telle liste peut s'avérer fastidieuse. Il aurait peut-être été plus réaliste

[78] Omer TENE, « For Privacy, European Commission Must Be Innovative », dans *Center For Democracy & Technology,* 2011, en ligne : <http://www.cdt.org/blogs/privacy-european-commission-must-be-innovative> (consulté le 23 mars 2011).
[79] *Supra* p. 5.

d'opérer le recensement des pays ne garantissant pas une protection adéquate ; et donc de dresser une liste noire. En plus de savoir si une législation est adéquate, on peut également se demander quel est le traitement réservé au suivi de la décision d'adéquation prise. En effet, comme le note Yves Poullet, il apparaît que *« la constatation de la conformité de contenu n'évacue pas la nécessité de s'assurer de l'effectivité du respect de celle-ci, peu importe la nature de la réglementation choisie et les institutions ou sanctions formellement mises en place par le pays étranger. 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 »*[80].

Enfin, il est régulièrement reproché la charge administrative et le coût de l'application de la directive 95. En matière de flux transfrontaliers, « *la plupart des responsables du traitement s'accordent à dire que l'obligation générale actuelle de notifier toutes les opérations de traitement aux autorités chargées de la protection des données est assez lourde et n'apporte pas, en soi, de réelle valeur ajoutée sous l'angle de la protection des données à caractère personnel* »[81]. Aussi certains n'hésitent pas à considérer que : « *The EU DPD is inundated with form filling and filing processes that currently occupy a vast ecosystem of regulators, data protection officers (DPOs), private sector lawyers, accounting firms, and consultants (to name a few). "Notifying" or registering data processing operations; approving cross border data transfers; executing "model clauses" or certifying "binding corporate rules" – are just some of the activities undertaken by privacy professionals »*[82].

Au delà du coût global de sa mise en œuvre, il convient également de passer en revue quelques unes des voies de contournements de la protection garantie par la directive de 95.

On peut ici relayer la place, paradoxalement néfaste, allouée au consentement dans l'architecture de la directive de 95. En effet, d'après le considérant 33, *« les données qui sont susceptibles par leur nature de porter atteinte aux libertés fondamentales ou à la vie privée ne devraient pas faire l'objet d'un traitement, sauf consentement explicite de la personne*

[80] Yves POULLET préc., note 10.
[81] Préc., note 18.
[82] Omer TENE préc., note 78.

concernée »[83]. De plus, l'article 26(1) de la directive de 95, « *lists several options which permit the export of personal data to a third country that does not have adequate protection. These options focus on the individual datasubject. The first situation is when the data subject gave unambiguous consent to the transfer. Consent is a crucial element of a data protection regime that is based on the notion of human dignity*»[84]. Il s'agit là, comme l'évoquent les Professeurs Trudel et Gautrais du « *Consentement* (utilisé) *comme sésame utilisable à la circulation des renseignements personnels »*[85]. Or dans bien des cas, le consentement n'est pas dépourvu « *d'ambiguïté »,* et pourrait même être qualifié d'illusoire dans les situations suivantes : « *The state does not need citizens' consent to process data about them; employers can obtain employee consent to anything save (perhaps) pay cuts; and businesses bury statements about privacy and data use in dense legal documents undecipherable to non-experts »*[86]. Par conséquent, il devient aisé d'envisager de contourner le niveau de protection offert par la directive de 95 en obtenant le consentement de la personne dont les données sont traitées. Or, dans biens des cas, les politiques de vie privée proposées sur Internet ont pour point commun d'être largement inintelligibles pour les utilisateurs, auxquels on demande de consentir.

A cela, il convient d'ajouter plusieurs difficultés introduites par de récentes évolutions technologiques. En effet, *« les modes de collecte de données à caractère personnel se complexifient et sont moins facilement décelables »*[87]. Selon Yves Poullet, « *l'approche suivie par la directive en ce qui concerne les flux transfrontalières est insuffisante au regard de la réalité actuelle des flux dans le contexte de notre société de l'information »*[88].

Enfin, parmi les voies de contournements susceptibles de limiter l'effectivité de la protection introduite par la directive de 95, on peut également citer le principe même du mécanisme du Safe Harbour, qui, comme nous l'avons observé, demeure facultatif pour les entreprises américaines. Aussi « *ironically, a company that has a privacy policy, or that certifies under the Safe Harbour Agreement, is subject to Federal Trade Commission (FTC) enforcement*

---

[83] Considérant 33 de la Directive de 95 préc., note 12.
[84] Michael D. BIRNHACK. "The EU Data Protection Directive: An Engine of a Global Regime" (2008), 24 *Computer Law & Security Report*.6 en ligne : http://works.bepress.com/michael_birnhack/14 (consulté le 23 mars 2011), p. 10.
[85] Vincent GAUTRAIS et Pierre TRUDEL, *Circulation des renseignements personnels et web 2.0,* Montréal, Édition Thémis, 2010, p. 163.
[86] Omer TENE préc., note 78.
[87] *Supra* note 18.
[88] Yves POULLET préc., note 10.

action, whereas a company without certification or a policy would not be »[89]. Ainsi, certaines entreprises américaines n'y adhérent pas et échappent par conséquent au contrôle qui en découle.

Cependant, la dimension optionnelle de ce cadre juridique est pourtant la rançon du consensus obtenu entre les américains et les européens. Certains considèrent d'ailleurs qu'en « *acceptant d'un côté, la méthode contractuelle et, de l'autre, en dégageant des principes contraignants, l'Union favorise l'émergence d'un équilibre, certes précaire, mais aussi symbolique de son influence dès lors qu'elle est unie »*[90].

En raison de la dimension globale de l'Internet, la gouvernance européenne en matière de protection des données ne peut être effective au sein de ses frontières qu'au prix d'un difficile consensus entre les États membres et ses partenaires internationaux qui est notamment illustré par les négociations houleuses de l'accord PNR entre les USA et l'UE.

2/ La difficulté d'élaborer un consensus tant au sein qu'à l'extérieur de l'Union européenne :

Au sein des frontières de l'UE les divergences demeurent, au point qu'en l'état, le cadre de la protection des données personnelles puisse donner l'impression d'un « *conglomérat disparate »* en raison des pratiques très hétérogènes qui restent celles des Etats membres. Il s'agit là d'un des travers de l'Union européenne qui peut être largement observé lorsque celle-ci légifère par voie de directive. Il en résulte, en dépit du cadre global de la directive de 95, une certaine disharmonie entre les solutions retenues au sein des frontières de l'Union. C'est pour cela que Peter Hustinx, le Contrôleur européen de la protection des données (CEPD) *« recently called for replacing the EU DPD with a regulation, European legislation with direct effect in Member States, to avoid the inevitable disharmony in transposition of a*

89 Adam TODD préc., note 30.
90 Xavier LATOUR, "Le droit communautaire et la protection des données à caractère personnel dans le commerce électronique." (2004), 27 *Petites affiches* 9, p.15.

directive. While an appealing prospect, such a regulation would be excruciatingly difficult to negotiate and agreed upon among 27 Member States »[91].

Si la recherche d'un cadre juridique global semble être aujourd'hui unanimement plébiscitée[92], il reste que la gouvernance européenne n'a pas encore atteint son point d'équilibre. A cet égard, l'émoi suscité par les négociations entre les Etats-Unis et l'Union européenne de l'accord PNR (*Passenger Name Records)*[93] est révélateur des dissensions qui dominent encore en la matière.

A la suite des attentats du 11 septembre 2001, le Congrès américain a adopté des mesures obligeant les compagnies aériennes à communiquer les données personnelles de leurs passagers au bureau des douanes et de la protection des frontières américain. Ces mesures ont confronté les compagnies européennes a un conflit de loi, puisque soumises, d'un côté, aux règles américaines et de l'autre, à la directive de 95 sur la protection des données[94]. Pour palier à cette insécurité juridique les USA et l'UE sont entrés en négociations. A la suite desquelles, la Commission a rendu une décision le 14 mai 2004 (2004/535/CE)[95], concluant que le *Department of Homeland Security Bureau of Customs and Border Protection* (CBP), était en mesure de garantir un niveau adéquat de protection pour les données transférées depuis la Communauté dans le cadre du PNR. Au regard de cette décision d'adéquation, le Conseil de l'Union européenne a approuvé la conclusion de l'accord PNR entre les Etats-Unis et la Communauté européenne par une décision du 17 mai 2004[96]. Finalement, le 28 mai 2004, était ratifié le premier accord PNR[97].

---

[91] Omer TENE préc., note 78.

[92] Voir *infra.* p. 25 et suivantes.

[93] Décision CE, *Décision 2007/551/CE du Conseil du 23 juillet 2007 relative à la signature, au nom de l'Union européenne, d'un accord entre l'Union européenne et les États-Unis d'Amérique sur le traitement et le transfert de données des dossiers passagers (données PNR) par les transporteurs aériens au ministère américain de la sécurité intérieure (DHS) (accord PNR 2007)* (2007), JO, PESC/JAI.

[94] Comme nous l'avons vu plus haut, avant l'entrée en vigueur du *Safe Harbour Agreement,* l'article 25 interdisait un transfert des données à un État tiers ne possédant pas un niveau adéquat de protection des données.

[95] Décision CE, *Décision 2004/535/CE, Commission Decision of 14 May 2004 on the adequate protection of personal data contained in the Passenger Name Record of air passengers transferred to the United States' Bureau of Customs and Border Protection* (2004) JO, L 235, Article 1, p. 11.

[96] Décision CE, *Décision 2004/496 du Conseil de l'Union européenne concernant la conclusion d'un accord entre la Communauté européenne et les États-Unis d'Amérique sur le traitement et le transfert de données PNR par des transporteurs aériens au bureau des douanes et de la protection des frontières du ministère américain de la sécurité intérieure,* JO, L 183 à la p. 83.

[97] *Agreement between the European Community and the United States of America on the processing and transfer of PNR data by air carriers to the United States Department of Homeland Security, Bureau of Customs and Border Protection, OJ* L 142M, 30.5.2004, p. 50.

Cet accord a eu pour conséquence d'allouer aux autorités américaines un large droit de regard sur les données personnelles des passagers européens. Ainsi, il a été critiqué par « *the European Parliament, humanitarian associations, and the Article 29 Data Protection Working Party for substantially having bypassed the Community principles concerning the protection of individual privacy and, in particular, for having violated the purpose limitation and the proportionality principles* »[98]. Aussi, le 27 juillet 2004, le Parlement européen, appuyé par le CEPD, ont intenté deux recours en annulation sur le fondement de l'article 230 CE[99], devant la CJCE[100], pour obtenir l'annulation de la décision du Conseil (n°496) et de celle d'adéquation de la Commission n°535. La CJCE, dans un jugement, du 30 mai 2006, a annulé les deux décisions précitées au motif que la décision d'adéquation (n°535) : « *involved the processing of personal data not falling within the scope of Directive 95/46 and, as a consequence, it infringed the Community norm itself* »[101]. En conséquence, la Cour a donc annulé l'accord PNR, obligeant à la conclusion d'un accord temporaire en octobre 2006[102], lequel a fait place, le 23 juillet 2007, à un accord définitif[103].

En dépit, des améliorations introduites dans la nouvelle mouture de l'accord, les autorités européennes chargées de la protection des données personnelles n'ont pas été rassurées. « *A l'instar du Contrôleur européen de la protection des données, la Commission informatique et libertés française (CNIL), a, par exemple, dénoncé la menace que fait peser l'accord sur de nombreuses garanties défendues par les CNIL européennes et « la surenchère américaine » opérée « au détriment des citoyens européens* ».[104]

---

[98] Michele NINO, "The Protection of Personal Data in the Fight Against Terrorism: New Perspectives of Pnr European Union Instruments in the Light of the Treaty of Lisbon.", M. (2010), 6 *Utrecht Law Review* 1 en ligne : < http://www.utrechtlawreview.org/index.php/ulr/article/viewFile/115/115>(consulté le 23 mars 2011), p.72.

[99] Art. 230, du Traité de Rome établissant la communauté européenne daté du 25 mars 1957.

[100] La Cour de justice de la communauté européenne (CJCE) est devenue depuis le Cour de justice de l'union européenne (CJUE).

[101] Joined Cases C-317/04 and C-318/04, *European Parliament* v. *Council of the European Union*, [2006] *ECR* I 4721. For an analysis of the judgment see G. Gilmore *et al.*, 'Court of Justice: Joined Cases C-317/04 and C 318/04, European Parliament v. Council and Commission', 2007 *Common Market Law Review*, no. 4, pp. 1081-1099.

[102] Décision CE, *Décision 2006/729/PESC/JAI du Conseil de l'Union européenne du 16 oct. 2006 relative à la signature, au nom de l'Union européenne, d'un accord entre l'Union européenne et les États-Unis d'Amérique sur le traitement et le transfert de données contenues dans les dossiers des passagers («données PNR») par des transporteurs aériens au ministère américain de la sécurité intérieure: JO L.298, à la p. 27-31.*

[103] *Agreement between the European Union and the United States of America on the processing and transfer of passenger name record (PNR) data by air carriers to the United States Department of Homeland Security*, *OJ* L 298, 27.10.2006, p. 2.

[104] CNIL, Conférence de presse du 09-07-2007, Présentation du 27ème rapport d'activité 2006 p.6.

Notons que l'accord est encore provisoirement appliqué, car depuis le traité de Lisbonne, il est requis le consentement du Parlement Européen pour être formellement conclu et conserver son effet juridique. Cependant, ce vote n'est toujours pas intervenu, à ce jour[105].

En s'opposant à ce que l'Union européenne « *be Serving its Citizens an American Meal* »[106], les réfractaires à l'accord PNR ont mis à jour la complexité des oppositions qui se jouent dans le « *polygone de force* » de la gouvernance de l'Union européenne en matière de protection des données. Compte tenu des critiques qui sont formulées à son endroit, notamment par de nombreux acteurs de la société civile[107], cet accord illustre la distance qui sépare encore l'approche américaine et européenne sur ces questions. Cet accord, et plus généralement la politique d'adéquation engagée par l'Union, semble davantage tenir du compromis que de l'exportation unilatérale de valeurs. Si certains auteurs avancent pourtant que *« from a data protection perspective, the EU managed to insert its principles into the policy calculations and mindset of reluctant counterparts »*[108], on se demandera, plutôt, si les difficultés liées à l'effectivité de ces mesures n'appellent pas, comme semble le plébisciter les acteurs de l'Union européenne, à l'érection d'un cadre global de la protection des données, voire à une entière réévaluation de la régulation de ce secteur.

B/ La recherche malaisée d'une solution globale :

À certains égards, l'action menée par l'Union européenne à propos des questions relatives à la protection des données peut être qualifiée d'unilatérale, tant l'Union est à l'initiative au plan international en la matière. Si comme nous l'avons observé plus haut, cette politique est parfois couronnée de succès, il convient pourtant de se représenter que le plus souvent ces réussites reposent sur la bonne volonté des acteurs qui y participent. Il est fait référence ici, aux entreprises qui acceptent de se soumettre aux *Safe Harbour principles,* aux États qui

---

[105] Communiqué de presse du Parlement européen, en date du 4 mars 2010 - 19:18, accessible en ligne : http://www.europarl.europa.eu/sides/getDoc.do?type=IM-PRESS&reference=20100301IPR69751&language=FR (consulté le 23 mars 2011).

[106] Cette citation est tirée du titre d'un article traitant de cette question dans Els De BUSSER, "EU Data Protection in Transatlantic Cooperation in Criminal Matters: Will the EU Be Serving its Citizens an American Meal?", (2010), 6 *Utrecht Law Review* 1.

[107] Je vous renvoie aux blogs publiés à cet égard sur les sites : www.laquadrature.net ou encore http://www.iris.sgdg.org.

[108] Michael D. BIRNHACK préc., note 84 p. 18.

acceptent d'assurer l'effectivité des législations homologuées et les exemples se multiplient ainsi.

En effet, plus encore que de s'interroger sur le fait de savoir si la législation européenne peut être réduite à une forme d'impérialisme juridique[109], il semble davantage pertinent de retenir ce nécessaire dialogue entre les ordres juridiques d'une part mais également d'autre part entre les différents acteurs qui participent à la mise en œuvre de cette gouvernance. Aussi, il semble que les grands chantiers de l'Union soient de deux ordres : poursuivre d'une part, le processus d'harmonisation législative au sein de l'Union (1) et prolonger d'autre part le processus de coopération au plan international (2). Cependant, en marge de ces deux chantiers, il semble qu'un mouvement soit engagé en Europe comme ailleurs, afin de faire émerger de nouvelles formes de régulation de la protection des données (autorégulation et promotion des technologies renforçant la protection de la vie privée)[110]. Ces dernières initiatives, plus conformes à un univers réseautique, nous servirons de propos conclusifs.

1/ La poursuite de l'harmonisation au sein de l'Union européenne :

La pertinence de la législation de l'Union européenne en matière de protection des données fait l'objet ces derniers mois d'un réexamen. La Commission a lancé à cet effet une révision du cadre juridique actuel ainsi qu'une large consultation publique.[111]. Parmi les problématiques soulevées à l'occasion de cette consultation on retrouve le souci : « *d'améliorer la cohérence du cadre juridique régissant la protection des données »,* ainsi : « *toutes les parties prenantes ont souligné la nécessité de disposer d'un instrument global, applicable aux opérations de traitement des données dans tous les secteurs et tous les domaines d'action de l'Union, garantissant une approche intégrée ainsi qu'une protection sans faille, cohérente et efficace »*[112].

---

[109] Voir les développements proposés à ce sujet par Yves POULLET préc., note 10.

[110] Voir notamment une communication de la Commission européenne visant à promouvoir la protection des données par les technologies renforçant la protection de la vie privée [COM(2007) 228 final - Non publiée au Journal officiel].

[111] Cette consultation a été clôturée à la fin de l'année 2009, pour voir les réponses à la consultation publique organisée par la Commission en ligne : http://ec.europa.eu/justice_home/news/consulting_public/news_consulting_0003_en.html (consulté le 20 mars 2011).

[112] Préc., note 46.

En effet, dans le prolongement du Traité de Lisbonne et de la disparition des piliers communautaires, il est devenu possible d'envisager un instrument global de protection embrassant tous les domaines d'action de l'Union européenne. Ainsi, par exemple, la coopération policière et la coopération judiciaire en matière pénale ne feraient plus l'objet d'un traitement à part[113]. Dorénavant, les principes de la directive de 95 auront vocation à être étendus aux domaines de la coopération policière et de la coopération judiciaires en matière pénale[114].

A côté de la création d'un cadre global, il est également envisagé de « *renforcer la dimension « marché intérieur » »*[115]. Cet objectif traduit le souci d'harmoniser les règles de protection des données au niveau de l'Union européenne. Ainsi, en matière de flux transfrontalier de données, les objectifs affichés par la réforme sont d'une part, d'uniformiser et de rendre plus cohérente l'approche à l'égard des pays tiers et des organisations internationales et d'autre part, de rationaliser les procédures actuelles. Sur ce deuxième point, il devient en effet urgent d'améliorer les procédures de transfert international de données qui, comme nous l'avons indiqué plus haut, se révèlent très lourdes financièrement pour une efficacité pratique encore trop relative.

Au delà de ces rationalisations, la réforme envisagée par l'Union européenne a vocation à assurer un niveau élevé de protection et de sécurité juridique aux personnes et entreprises présentes dans le marché intérieur. Les questions de la régulation des technologies et du consensus internationale demeurent au centre de la réflexion engagée à propos du cadre global proposé. A cet égard, on peut considérer que la Commission embrasse une position très, voire trop volontariste. En effet, la Commission précise que « *peu importe la complexité de la situation ou le caractère sophistiqué de la technologie, il est essentiel que les règles et les normes applicables, que les autorités nationales doivent faire appliquer et auxquelles les entreprises et les développeurs de technologies doivent se conformer, soient définies*

[113] L'article 16 du traité sur *le fonctionnement de l'Union européenne* (TFUE) « *instaure une nouvelle base juridique qui permet notamment à l'Union de réglementer la protection des données au moyen d'un seul instrument juridique, notamment dans le domaine de la coopération policière et de la coopération judiciaire en matière pénale* » dans préc., note 18.

[114] La Commission a, en effet, annoncé son intention d'examiner l'opportunité d'étendre l'application es règles de ces règles de protection, sous réserves de certaines exceptions (droit d'accès, ou le principe de transparence). Préc., note 18 p. 16.

[115] Préc., note 18 p. 11

clairement »[116]. On s'interrogera ici, sur le fait de savoir s'il est seulement possible de se défaire de ces contingences technologiques.

Le récent développement, par exemple, du « *Cloud computer »,* c'est-à-dire l' « *informatique en nuage* » constitue un véritable défi pour la protection des données car il signifie pour le particulier « *une perte de contrôle sur les informations potentiellement sensibles qui le concernent, lorsqu'il stocke ses données à l'aide de programmes hébergés sur l'ordinateur d'autres personnes »*[117].

Ce type d'avancée technologique révèle encore une fois le lien étroit qui caractérise la relation entre données personnelles et Internet. En ce sens, vouloir garantir un niveau de protection aux ressortissants de l'UE, suppose de prendre la mesure des défis technologiques, lesquels, induisent ici *« un défi international »*[118]. En raison de la dimension internationale de l'Internet, les États, ou les ensembles régionaux telle que l'Union européenne, ne peuvent plus se réfugier « *derrière des lois divergentes* (…) *en réactualisant des frontières virtuelles en lieu et place des frontières physiques »*[119]. L'union européenne ne peut garantir un haut niveau de protection qu'au terme d'un fort consensus international sur ces questions.

2/ La fréquence supranationale porteuse de solutions :

Toute tentative d'améliorer le niveau de protection assuré au sein du marché intérieur se voit irrémédiablement contrecarré si un tel objectif n'est pas partagé par les partenaires de l'Union européenne.

À l'occasion de la Conférence Internationale des Commissaires à la Protection des Données et de la Vie Privée en date du 29 novembre 2010 *« les autorités de protection des données du monde entier ont souligné l'urgence d'adopter rapidement une convention internationale dans le domaine de la protection des données personnelles »*[120]. Comme évoquée à cette occasion, l'augmentation des transferts internationaux de données personnelles suppose d'élaborer des « *règles*

[116] *Id.*
[117] Préc., note 18 p. 2
[118] Préc., note 47.
[119] Yves POULLET préc., note 10.
[120]Le projet de résolution est en ligne : http://www.cnil.fr/fileadmin/documents/approfondir/dossier/international/2010-conf_itlee_resolution_projet_FR.pdf (consulté le 23 mars 2011).

internationales qui garantissent d'une façon uniforme le respect de la protection des données »[121]. Compte tenu de l'interdépendance des économies dans le cadre des réseaux d'information, la question de la gouvernance de la protection de données personnelles ne peut plus, sous peine d'ineffectivité, être conçue unilatéralement. Dans plusieurs hypothèses on ne sait toujours pas quel droit appliquer lorsque plusieurs établissements d'une multinationale sont implantés dans différents Etats. Il est devenu indispensable d'élaborer des normes globales internationales.

Plusieurs initiatives positives ont été prises par différentes organisations internationales afin de déterminer des standards internationaux communs. Il s'agit notamment, et de façon non exhaustive, de rappeler les actions entreprises par « *l'OCDE, par le Conseil de l'Europe, par l'APEC, par l'UNESCO, par l'Organisation internationale de la Francophonie, par la Communauté Economique des Etats de l'Afrique de l'Ouest (CEDEAO), par l'Organisation internationale de la Normalisation (ISO), ou encore par le Forum sur la gouvernance de l'Internet. Les travaux des groupements d'autorités de protection des données, tels que le Réseau ibéro-américain de protection des données personnelles (RIPD), l'Association francophone de protection des données personnelles (AFAPDP), le Forum des autorités de protection de la vie privée de l'Asie et du Pacifique (Forum APPA) et le Réseau global pour le respect de la vie privée (GPEN) »*[122].

L'effectivité du modèle de protection des données personnelles défendu par l'Union européenne, passe nécessairement par une coopération avec les pays tiers (USA certes mais également la Chine etc.) et les organisations internationales tels que l'OCDE, le Conseil de l'Europe, les Nations unies, et d'autres organisations régionales.

Propos conclusifs : Vers une solution réseautique ?

Comme nous l'avons vu, l'Union européenne s'est engagée afin de protéger son modèle de protection des données dans une dynamique législative ambitieuse qui a eu de nombreuses répercussions au plan international.

[121] Préc., note 120.
[122] Préc., note 120, voir également les développements apportés à ce sujet par Marie Georges préc., note 47.

On l'a vu, cette politique fait davantage référence à la notion de « *gouvernance* », telle que développée par Jacques Chevalier, en raison des nombreux acteurs qui y participent. Si elle reprend certaines voies d'actions traditionnelles (directive, Chartes des droits et libertés fondamentaux), on observe cependant qu'elle défriche un grand nombre de nouvelles modalités de régulation (les BCR, les clauses contractuelles types et autres). On peut voir ici le laboratoire de ce que pourraient être d'autres politiques extérieures de l'Union européenne à l'avenir.

Ces nouvelles formes de régulation placent au centre les multinationales, telles des véhicules, à l'échelle planétaire, de la diffusion de la protection des données personnelles. Cette perspective a pour mérite de resituer les multinationales dans le processus décisionnel de l'Union européenne et d'intégrer la pluralité des foyers de normativités qui s'agencent à côté des ordres juridiques nationaux, régionaux et internationaux. Cette perspective, plus conforme à l'analyse en réseau[123], laisse tout de même en suspens, comme nous l'avons vu, certaines questions fort pertinentes quant à l'effectivité de la protection formulée.
Ainsi, et plus généralement, on est en droit de s'interroger sur la pertinence d'une solution juridique apportée en réponse à des bouleversements d'ordre technologique. Peut être est-il venu le temps d'agencer aux mécanismes juridiques certains dispositifs techniques visant au développement de technologies renforçant la protection de la vie privée[124].

Se pourrait-il que le nouveau paradigme ne soit plus « *data protection by law* » mais « *data protection by design* » ?

[123]François OST et M Van de KERCHOVE, *De la pyramide au réseau ? : pour une théorie dialectique du droit,* Bruxelles, Presses des Facultés Universitaires Saint Louis, 2002.
[124] Peter HUSTINX « Respect de la vie privée dès la conception (Privacy by Design): le séminaire définitif» Madrid, le 2 novembre 2009 <http://www.edps.europa.eu/EDPSWEB/webdav/shared/Documents/EDPS/Publications/Speeches/2009/09-11-02_Madrid_privacybydesign_FR.pdf> (consulté le 20 mars 2011).

Bibliographie

Sites Internet

- www.cnil.fr
- www.cnpd.public.lu
- http://ec.europa.eu
- www.export.gov
- www.iris.sgdg.org.
- www.laquadrature.net
- www.privacycommission.be

Législations et réglementations

Accords internationaux

- *Accord Passenger Name Record (PNR), OJ* L 142M, 30.5.2004, p. 50.

Législation du Conseil de l'Europe

- *Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel Strasbourg*, 28 janvier 1981, (1981) S.T.E. n° 108.

Législations de l'Union européenne

- Traité sur *le fonctionnement de l'Union européenne* (TFUE)
- *Charte des droits fondamentaux de l'union européenne* disponible en ligne : <http://www.europarl.europa.eu/charter/pdf/text_fr.pdf> (consulté le 23 mars 2011)
- Directive CE, directive 95/46/CE *du Parlement européen et du Conseil, du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données* (1995) JO, L 281 à la p. 31

Décisions du Conseil de l'Union européenne

- Décision CE, *Décision* 2000/520/CE de la Commission du 26 juillet 2000 faisant suite à la Directive 95/46/CE du Parlement européen et du Conseil *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 États-Unis d'Amérique* JO, L215 à la p7.

- Décision CE, *Décision 2004/496 du Conseil de l'Union européenne concernant la conclusion d'un accord entre la Communauté européenne et les États-Unis d'Amérique sur le traitement et le transfert de données PNR par des transporteurs aériens au bureau des douanes et de la protection des frontières du ministère américain de la sécurité intérieure,* JO, L 183 à la p. 83.

- Décision CE, *Décision 2006/729/PESC/JAI du Conseil de l'Union européenne du 16 oct. 2006 relative à la signature, au nom de l'Union européenne, d'un accord entre l'Union européenne et les États-Unis d'Amérique sur le traitement et le transfert de données contenues dans les dossiers des passagers («données PNR») par des transporteurs aériens au ministère américain de la sécurité intérieure: JO L.298, à la p. 27-31.*

- Décision CE, *Décision 2007/551/CE du Conseil du 23 juillet 2007 relative à la signature, au nom de l'Union européenne, d'un accord entre l'Union européenne et les États-Unis d'Amérique sur le traitement et le transfert de données des dossiers passagers (données PNR) par les transporteurs aériens au ministère américain de la sécurité intérieure (DHS) (accord PNR 2007) (*2007), JO, PESC/JAI.

Décisions de la Commission européenne

- Décision CE, *Décision* 2000/520/CE de la Commission du 26 juillet 2000 faisant suite à la Directive 95/46/CE du Parlement européen et du Conseil *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 États-Unis d'Amérique* JO, L215 à la p7.

- Décision CE, *Décision 2001/497/CE de la Commission du 15 juin 2001 relative aux Clauses contractuelles types pour le transfert de données à caractère personnel vers des pays tiers en vertu de la directive 95/46/CE* (2001), JO L181 à la p. 19

- Décision CE, *Décision 2002/16/CE de la Commission du 27 décembre 2001 relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des sous-traitants établis dans des pays tiers en vertu de la directive de 95/46* (2002), JO L 281 du 23.11.1995, p. 31.

- Décision CE, *Décision 2004/535/CE, Commission Decision of 14 May 2004 on the adequate protection of personal data contained in the Passenger Name Record of air passengers transferred to the United States' Bureau of Customs and Border Protection* (2004) JO, L 235, Article 1, p. 11.

- Décision CE, *Décision 2011/61/CE de la Commission du 31 janvier 2011 constatant, conformément à la directive 95/46/CE du Parlement européen et du Conseil, le niveau de protection adéquat des données à caractère personnel assuré par l'État d'Israël concernant le traitement automatisé des données à caractère personnel,* (2011) JO L 281 à la p. 31.

Communications de la Commission européenne

- COMMISSION EUROPEENNE *Une approche globale de la protection des données à caractère personnel dans l'Union européenne,* 4 novembre 2010, disponible en ligne <http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_fr.pdf> (consulté le 23 mars 2011).

Jurisprudences

- CJUE C-317/04 *European Parliament* v. *Council of the European Union*, [2006] *ECR* I 4721
- CJUE C-318/04, European Parliament v. Council and Commission.

Doctrine

Monographies

- CHEVALIER, J. *L'Etat post-moderne,* Paris, L.G.D.J. (2008)

- GAUTRAIS, V. and P. TRUDEL, *Circulation des renseignements personnels et web 2.0,* Montréal, Édition Thémis, 2010

- HABERMAS J, *Droit et Démocratie — Entre faits et normes*, traduit de l'anglais par R. Rochlitz et C. Bouchindhomme, Paris, Gallimard, 1997

- OST, F. and M. VAN-DE-KERCHOVE *De la pyramide au réseau ? : pour une théorie dialectique du droit,* Bruxelles, Presses des Facultés Universitaires Saint Louis, 2002.

Articles de revue et études d'ouvrages collectifs

- BALI, V. (2006). "Data privacy, Can India Provide Adequate Protection for Electronically Transferred Data ?" bepress Legal Series. Working Paper 1594 en ligne : http://law.bepress.com/expresso/eps/1594 (consulté le 23 mars 2011).

- BENNETT, C. J, *"*Convergence Revisited: Toward a Global Policy for the Protection of Personal Data*",* dans Philip E. AGRE et Marc ROTENBERG *Technology and privacy* Cambridge, The New Landscape. Cambridge, MA: MIT Pres, 1997, p. 99.

- BIRNHACK, M. D. "The EU Data Protection Directive: An Engine of a Global Regime" (2008), 24 *Computer Law & Security Report*.6 en ligne : http://works.bepress.com/michael_birnhack/14 (consulté le 23 mars 2011)

- BUSSER, E. D. "EU Data Protection in Transatlantic Cooperation in Criminal Matters: Will the EU Be Serving its Citizens an American Meal?", (2010), 6 *Utrecht Law Review* 1.

- CATE, F. H. "The Changing Face of Privacy Protection in the European Union and the United States" (1999) 33-173 *Indiana Law Rev*, en ligne<http://ssrn.com/paper=933090> *abstract* (consulté le 23 mars 2011).

- DAVOLI, A. "Protection des données à caractère personnel", (2010) en ligne : < http://www.europarl.europa.eu/ftu/pdf/fr//FTU_4.12.8.pdf> (consulté le 22 mars 2011)

- FARRELL, H. "*Constructing the International Foundations of E-Commerce - The E.U - U.S. Safe Harbour Arrangement* " (2003), 57 *Int'L Organisation* 277

- LATOUR, X., "Le droit communautaire et la protection des données à caractère personnel dans le commerce électronique." (2004), 27 *Petites affiches* 9,.

- NINO, M. "The Protection of Personal Data in the Fight Against Terrorism: New Perspectives of Pnr European Union Instruments in the Light of the Treaty of Lisbon.", M. (2010), 6 *Utrecht Law Review* 1 en ligne : < http://www.utrechtlawreview.org/index.php/ulr/article/viewFile/115/115>(consulté le 23 mars 2011).

- POULLET, Y. "Comment appliquer les règles de protection des données aux transfert de données personnelles dans une société à la fois globale mais également multi-économique et multiculturelle ?" (2007) 12-1 *Lex Electronica* en ligne : <http://www.lex-electronica.org/docs/articles_33.pdf> (consulté le 23 mars 2011).

- QUILLATRE, E, « La libre circulation des données à caractère personnel au sein du marché intérieur et de l'ELSJ et nouveaux outils de régulation », (2011), 24 *Les petites affiches* 10

- TENE, O. « For Privacy, European Commission Must Be Innovative *»,* dans *Center For Democracy & Technology,* 2011, en ligne : <http://www.cdt.org/blogs/privacy-european-commission-must-be-innovative> (consulté le 23 mars 2011).

- THOMAS-SERTILLANGES, J.-B. "Libre circulation des données à caractère personnel et protection de la vie privée, entre marché intérieur et ELSJ", (2011), 24 *Les petites affiches* 3

- TODD, A. G. "Painting a Moving Train: Adding "Postmodern" to the Taxonomy of Law "(2008) 40 *The University of Toledo Law Review* 105, p 136, citant James Q. WHITMAN, "The Two Western Cultures of Privacy : Dignity versus Liberty", (2004), 113 *Yale Law Journal*. 1151

Documents internationaux

- UNESCO, *Le droit fondamental des personnes à la protection des données personnelles: les défis à relever sur le plan national, régional et mondial,* discours prononcé par Marie Georges, Conseiller pour la prospective et pour le développement du président de la Commission nationale de l'informatique et des libertés (CNIL), (Paris 2007) en ligne : < http://portal.unesco.org/ci/en/files/26953/12121570985Georges-Marie.pdf/Georges-Marie.pdf> (consulté le 23 mars 2011).

Index