Le transfert de données à caractère personnel vers les Etats-Unis conformément au droit européen

Moal, Carole

Published in:
Revue trimestrielle de droit européen

Publication date:
2002

Document Version
le PDF de l'éditeur

Le transfert de données à caractère personnel vers les Etats-Unis conformément au droit européen

Carole MOAL-NUYTS

Membre du Barreau de New York
Jones Day Reavis & Pogue, Bruxelles

En vue de se conformer aux prescriptions de la directive 95/46/CE relative à la protection des personnes physiques à l'égard des données à caractère personnel, les entreprises désireuses de transférer des données vers les Etats-Unis ont à leur disposition plusieurs options. L'étude procède à l'examen des deux systèmes principaux que sont le *Safe Harbor* et les Clauses contractuelles types.

1. Depuis l'adhésion du géant Microsoft, le 29 juin 2001, au système américain de protection des données à caractère personnel, connu sous le nom de *Safe Harbor* (ou « sphère de sécurité »), ce système semble avoir pris son essor, démentant ainsi les prédictions de ceux qui le voyaient déjà tomber en désuétude pour cause de non-adhésion (1). Officiellement opérationnel depuis le 1er novembre 2000, le *Safe Harbor* compte, au 1er janvier 2002, plus de cent cinquante entreprises américaines adhérentes (2). Elaboré sous l'égide du ministère du Commerce des Etats-Unis (*US Department of Commerce*) et de la Commission européenne, le système fait suite à l'entrée en vigueur de la 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 (ci-après « la directive ») (3).

En vertu de la directive, les Etats membres sont tenus de veiller à ce que les transferts de données à caractère personnel vers un pays tiers n'aient lieu que si le pays en question assure un *niveau de protection adéquat* (4). Or, compte tenu de la divergence de conception de la protection des données à caractère personnel en Europe et aux Etats-Unis, le système américain n'a pas été jugé suffisamment

(1) V. notamment S. Huart, Les *Safe Harbor principles* ou les Principes de la sphère de sécurité, DA OR Actualité, 2000-2001.16.

(2) V. la liste des adhérents, disponible sur le site internet du ministère du Commerce américain à l'adresse suivante : <http ://web.ita.doc.gov/safeharbor/shlist.nsf/webPages/safe%20harbor%20list !>.

(3) JOCE L 281, 23 nov. 1995, p. 31.

(4) Art. 25(1) de la directive.

sûr pour justifier d'une reconnaissance de niveau de protection adéquat au sens de la directive. En effet, tandis que les Etats-Unis s'en remettent de manière générale à l'autorégulation par les entreprises ou tout au plus à une réglementation sectorielle (5), l'Union européenne, considérant la protection des données à caractère personnel comme un droit fondamental, préfère quant à elle la voie de la réglementation impérative, comme en témoigne la directive (6). Le gouvernement américain a pris très au sérieux la menace que représentait le nouveau régime européen pour le transfert de données au départ de l'Europe vers les Etats-Unis, ces derniers s'avérant être la destination d'un nombre important de transferts de données au départ d'Etats membres de l'Union européenne (7).

Ce n'est qu'au terme d'une longue négociation dans un climat de conflit commercial (8), que les Etats-Unis et la Commission européenne sont finalement parvenus, en juin 2000, à s'accorder sur le système du *Safe Harbor,* lequel repose sur des principes de protection des données personnelles auxquels peuvent adhérer les entreprises américaines, et que la Commission a jugé adéquats.

Alors que le système du *Safe Harbor* venait à peine d'être mis en place, la Commission a pris une nouvelle initiative dans cette matière. Conformément au mandat qui lui est donné par la directive, elle a adopté des *Clauses contractuelles types* auxquelles les entreprises peuvent se référer, sur une base volontaire, et qui sont réputées offrir des garanties suffisantes lors du transfert de données à caractère personnel vers des pays tiers. C'est donc à présent deux systèmes optionnels supplémentaires distincts qui sont mis à la disposition des entreprises américaines qui envisagent de transférer des données à caractère personnel au départ de l'Union européenne.

2. La présente étude a pour objet d'examiner dans quelle mesure les sociétés européennes, qu'elles soient des filiales de sociétés américaines ou autres, peuvent désormais transférer des données à caractère personnel à destination des Etats-Unis, conformément au droit européen. Après avoir rappelé les principes fondamentaux de la directive relatifs au transfert de données à caractère personnel vers des pays tiers à l'Union européenne (I), l'on examinera le régime du *Safe Harbor* (II), puis celui des clauses contractuelles types (III). L'on pourra alors, en guise de conclusion, porter une appréciation globale sur l'avenir de ces deux systèmes.

(5) V. Annexe I de la décision de la Commission du 26 juillet 2000 conformément 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 Etats-Unis d'Amérique, JOCE L 215, 25 août 2000, p. 7.

(6) L'on a parlé à cet égard de « choc de cultures juridiques » (*clash of legal cultures*) : V. la citation du député européen D. Wallis, Parliament's threatens legal action, calls safe harbor deal inadequate, World Telecom Law Report, 2000.23.

(7) Nombre qui n'a eu cesse de croître depuis l'apparition des nouvelles technologies de l'information et la globalisation de l'économie. V. S. Huart, *op. cit.* (note 1), p. 14.

(8) V. P. Thieffry, L'émergence d'un droit européen du commerce électronique, RTD eur. 2000.649, spéc. p. 650.

I. – LES PRINCIPES DE LA DIRECTIVE 95/46/CE

3. Entrée en vigueur le 24 octobre 1998, la directive a été transposée, jusqu'à présent dans le droit de douze Etats membres (9). La directive s'inspire de divers instruments internationaux (10), et spécialement de la convention n° 108 du Conseil de l'Europe (11). L'objectif fondamental de la directive est d'assurer le respect des libertés et droits fondamentaux des personnes lors du traitement des données à caractère personnel (12). Les dispositions de la directive s'inspirent d'un certain nombre de principes fondamentaux parmi lesquels on retiendra surtout la limitation des transferts autorisés à ceux qui ont une finalité spécifique, la transparence, la sécurité, les droits d'accès, de rectification et d'opposition et les restrictions aux transferts ultérieurs (13). Le transfert de données à caractère personnel vers des pays tiers, qui nous intéresse plus particulièrement dans le cadre de la présente étude, fait l'objet du chapitre IV de la directive.

4. Disposition essentielle de ce chapitre IV de la directive, l'article 25, § 1er instaure le principe de *garantie du niveau de protection adéquat,* qui veut qu'un transfert vers un pays tiers de données à caractère personnel destinées à faire l'objet d'un traitement après leur transfert ne peut avoir lieu que si le pays tiers assure un niveau de protection adéquat.

Pour décider si le pays tiers assure un niveau de protection adéquat, il y a lieu, précise le paragraphe 2 de la même disposition, d'avoir égard à toutes les circonstances entourant le transfert, et notamment à *la finalité et la durée* des traitements envisagés, à l'identité des pays d'origine et de destination finale, aux *règles de droit,* générales ou sectorielles, en vigueur dans le pays tiers en cause, ainsi qu'aux *règles professionnelles* et aux mesures de sécurité qui y sont respectées.

(9) Après avoir adressé le 29 juillet 1999 un avis motivé à neuf Etats membres, pour non-communication des mesures nécessaires à la transposition de la directive, la Commission a finalement engagé une action en justice, le 11 janvier 2000, contre la France, le Luxembourg, les Pays-Bas, l'Allemagne et l'Irlande. Depuis lors, des législations transposant la directive sont entrées en vigueur en Allemagne et aux Pays-Bas. Des projets de lois ont été élaborés en France, en Irlande et au Luxembourg. Pour plus de détails, V. le tableau dressé par la Commission sur l'état de transposition de la directive, disponible à l'adresse internet suivante : <http ://europa.eu.int/comm/internal_market/en/dataprot/law/impl.htm>. Comme la Commission l'a elle-même souligné, les particuliers peuvent conformément à la jurisprudence *Marleasing* de la Cour de justice, faire valoir certaines des dispositions de la directive devant les juridictions nationales de ces Etats. En outre, conformément à la jurisprudence *Francovich,* les particuliers ayant subi un préjudice en raison de la non-transposition de la directive peuvent, dans certains cas, solliciter une compensation devant les juridictions nationales. V. La Commission engage une action en justice contre cinq Etats membres, Commission européenne, 11 janv 2000, <http ://www.europa.eu.int/comm/internal_market/fr/dataprot/news/2k-10.htm>.

(10) Et notamment des Lignes directrices de l'OCDE régissant la protection de la vie privée et les flux transfrontières de données à caractère personnel, Paris, OCDE, 1981.

(11) Convention du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, Série des traités européens, n° 108. V. le Document de travail du 24 juillet 1998 du Groupe de protection des personnes à l'égard du traitement des données à caractère personnel, (« Transfert de données à caractère personnel à des pays tiers : application des articles 25 et 26 de la directive européenne relative à la protection des données », <http ://www.europa.eu.int/comm/internal market/en/dataprot wpdocs/wp12fr.pdf>), ci-après, « Document de travail du Comité 29 », p. 5.

(12) V. considérants 1 et 2.

(13) V. Document de travail du Comité 29, *op. cit.* (note 11) p. 6-7.

Ainsi que le Parlement l'a souligné, il n'est pas obligatoire, pour que le pays tiers soit réputé assurer un niveau de protection adéquat que ledit pays dispose de règles analogues à celles de l'Union, mais il faut que la personne concernée *soit protégée de manière effective,* quel que soit le type de protection juridique en vigueur dans ce pays (14).

Dans ses réflexions et recommandations relatives à l'interprétation de l'article 25, le Comité relatif à la protection des personnes à l'égard du traitement des données à caractère personnel institué en vertu de l'article 29 de la directive (ci-après « le Comité 29 ») (15) a, quant à lui, précisé que *toute analyse sérieuse du niveau de protection adéquat doit s'intéresser aux deux éléments fondamentaux suivants : le contenu des règles applicables et les moyens d'assurer le respect de ces règles* (16).

5. En vertu de la procédure instituée par la directive, les Etats membres et la Commission s'informent mutuellement des situations dans lesquelles ils estiment qu'un pays tiers n'assure pas un niveau de protection adéquat (17), et lorsque la Commission constate, selon la procédure prévue par la directive, qu'un pays tiers n'assure pas un tel niveau de protection, les Etats membres doivent prendre les mesures nécessaires en vue d'empêcher tout transfert de données vers ce pays (18). Assistée du Comité 29, la Commission peut constater qu'un pays tiers remplit le critère de protection adéquate. Cette constatation permet de transférer des données personnelles vers le pays en question sans qu'aucune garantie additionnelle ne soit exigée.

A ce jour, seuls les régimes de protection des données personnelles suisse, hongrois, canadien et du *Safe Harbor* américain ont été reconnus comme offrant une protection adéquate (19). Selon ses propres estimations, la Commission n'envisage de reconnaître comme adéquats au sens de la directive que les régimes d'un nombre limité de pays (20). Ce qui accroît d'autant l'intérêt du système de dérogation à l'article 25 de la directive qui est prévu à son article 26.

(14) V. Résolution du Parlement européen sur le projet de décision de la Commission relative à la pertinence des niveaux de protection fournis par les principes de la sphère de sécurité et les questions souvent posées y afférentes, publiées par le ministère du Commerce des Etats-Unis », doc. n° A5-0177/2000, (ci-après, « La résolution du Parlement européen sur le *Safe Harbor* »), point B b) <http ://www3.europarl.eu.int/omk/omnsapir.so/pv2?APP=PV2&PRG=CALEND&FILE=000705&TPV=DEF&LANGUE=FR>.

(15) Ce Comité est chargé de donner à la Commission un avis sur le niveau de protection dans la Communauté et dans les pays tiers : V. art. 30 de la directive.

(16) V. Document de travail du Comité 29, *op. cit.* (note 11), p. 5. V. également Y. Poullet, Les *Safe Harbor Principles* – Une protection adéquate ?, <http ://www.droit-technologie.org>, p. 8.

(17) Art. 25(3) de la directive.

(18) Art. 25(4) de la directive.

(19) La Suisse et la Hongrie disposant de lois d'application générale sur la protection des données qui suivent globalement la même approche que la directive, la décision d'admettre que ces pays assurent un niveau de protection adéquat a été relativement facile et concerne tous les transferts de données à caractère personnel vers ces pays. Tandis que dans le cas des Etats-Unis, comme exposé ci-après, le caractère adéquat n'est reconnu qu'aux seules entreprises ayant adhéré au *Safe Harbor*. V. respectivement, les décisions de la Commission 2000/518/CE (Suisse), 2000/519/CE (Hongrie), 2000/520/CE (USA) du 26 juill. 2000, JOCE L 215, 25 août 2000. Quant au Canada, son système de protection des données n'a été reconnu comme assurant une protection adéquate qu'à la suite de l'adoption de la loi interne sur la protection des renseignements personnels et les documents électroniques. V. décis. de la Commission 2002/ 2/CE, JOCE L 2, 4 janv. 2002.

6. L'article 26 de la directive prévoit diverses possibilités pour transférer de manière licite des données à caractère personnel vers des pays tiers dont le régime de protection n'est pourtant pas jugé « adéquat » au sens de la directive. Le paragraphe 1er de cette disposition donne une liste de six situations où le transfert de données sera considéré comme licite. Ainsi que le Comité 29 l'a souligné, les dérogations ainsi aménagées sont formulées *de manière restrictive* et concernent, pour l'essentiel, des cas où les risques pour la personne concernée sont relativement faibles ou des situations dans lesquelles d'autres intérêts (qu'ils soient publics ou propres à la personne concernée elle-même) priment le droit de la personne concernée au respect de la vie privée. En outre, les Etats membres peuvent prévoir dans leur droit national que ces dérogations ne s'appliqueront pas dans certains cas qu'ils déterminent (21). Chacune des six dérogations est examinée brièvement dans les lignes qui suivent.

7. La première dérogation est prévue à la lettre (a) de l'article 26(1), qui autorise le transfert lorsque la personne concernée a *indubitablement donné son consentement* audit transfert. Conformément à l'article 2, point h) de la directive, ce consentement doit être *libre, spécifique et informé.* Le Comité 29 a souligné que l'exigence d'information impliquait que la personne concernée *soit correctement informée du risque spécifique que les données la concernant soient transférées vers un pays n'assurant pas une protection adéquate* (22). De l'exigence du caractère indubitable du consentement, il ressort que le moindre doute sur le fait qu'il a bien été donné rendrait la dérogation inapplicable. En pratique, les rédacteurs du formulaire de consentement devront veiller à ce que le consentement soit donné de manière claire et non équivoque. On observera que la preuve du caractère *libre* du consentement pourrait s'avérer délicate dans le cas où celui-ci serait requis d'un employé engagé dans un lien de subordination vis-à-vis de la personne l'ayant recueilli (23).

8. Les deuxième et troisième dérogations visent le cas où le transfert est nécessaire à la conclusion ou l'exécution d'un *contrat* entre la personne concernée et le responsable du traitement ou entre le responsable du traitement et un tiers (24). Nonobstant le caractère apparemment vaste de ces deux dérogations, leur application en pratique demeure fortement limitée par le critère de *nécessité.* Dès lors que des données non essentielles à l'exécution du contrat sont trans-

(20) V. le considérant 4 de la décision 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, décis. C(2001)497 CE, JOCE L 181/19, 4 juill. 2001. La Commission a également entamé des discussions avec plusieurs autres pays tiers, dont notamment l'Australie et le Japon

(21) V. Document de travail du Comité 29, *op. cit.* (note 11), p. 25.

(22) V. Document de travail du Comité 29, *op. cit.* (note 11), p. 25.

(23) V. Document de travail du Comité 29, *op. cit.* (note 11), p. 25. A notre avis, il n'est pas certain que l'obstacle pourrait être contourné simplement par l'obtention d'une déclaration explicite de l'employé selon laquelle le consentement a été donné librement et en connaissance du fait que le refus de donner le consentement n'aurait entraîné aucune sanction.

(24) Lettres (b) et (c) de l'art. 26(1).

férées, ou que le transfert répond à une autre finalité que l'exécution stricte du contrat, la dérogation s'avérera inapplicable (25). Ainsi, il est vraisemblable que les transferts de données personnelles d'employés d'une entreprise dont le bureau de management du personnel se trouverait dans un pays tiers ne pourraient bénéficier de la dérogation, dans la mesure où ces transferts ne paraissent pas résulter d'une nécessité mais simplement d'une convenance. En revanche, devraient répondre au critère de nécessité, des transferts de données personnelles par exemple lors de la réservation d'un billet d'avion, ou d'une chambre d'hôtel, effectués par l'agent de voyage lors de la réservation d'un voyage pour son client. L'on peut encore penser aux transferts de données personnelles nécessaires aux opérations de paiement international par carte bancaire ou par carte de crédit (26).

9. La quatrième dérogation concerne le cas où le transfert est nécessaire ou rendu juridiquement obligatoire *pour la sauvegarde d'un intérêt public important ou* pour *la constatation, l'exercice ou la défense d'un droit en justice* (27). Par transferts *nécessaires* pour la sauvegarde d'un intérêt public important, il faut entendre les transferts entre administrations publiques, tels les échanges de données entre les administrations fiscales ou douanières, entre les services de sécurité sociale, ou encore entre les autorités de surveillance du secteur des services financiers (28). Par transferts *rendus juridiquement obligatoires* pour la sauvegarde d'un intérêt public important ou la défense d'un droit en justice, l'on vise les transferts effectués dans le cadre de procédures judiciaires internationales (29).

10. La cinquième dérogation a trait à l'hypothèse où le transfert s'avère nécessaire pour *la sauvegarde de l'intérêt vital de la personne concernée* (30). Conformément au considérant 31 de la directive, l'intérêt vital de la personne concernée doit s'interpréter au sens strict, à savoir comme *un intérêt essentiel à la vie de la personne concernée.* Sont ainsi exclues les autres formes d'intérêts, tels les intérêts financiers, patrimoniaux ou familiaux (31). Cette exception est en fait destinée à couvrir des transferts urgents de données personnelles à des fins médicales, dans l'hypothèse où la personne concernée serait dans l'impossibilité de donner son consentement (32). On songe par exemple au cas où la personne concernée serait inconsciente au moment où le consentement devrait normalement être donné et où l'exception prévue à la lettre (a) (*supra,* n° 7) ne pourrait jouer.

11. La sixième et dernière situation où le transfert est autorisé vers un pays tiers dont le régime de protection des données n'est pas adéquat au sens de la directive, est celle où ledit transfert intervient *au départ d'un registre public.* Il ne s'agit

(25) V. Document de travail du Comité 29, *op. cit.* (note 11), p. 25.
(26) V. Document de travail du Comité 29, *op. cit.* (note 11), p. 25. V. également Cullen International, A business guide to changes in European Data protection legislation, Kluwer Law International, 1999, p. 100-101.
(27) Lettre (d) de l'art. 26(1).
(28) V. considérant 58 de la directive. V. égal. le Document de travail du Comité 29, *op. cit.* (note 11), p. 26.
(29) V. Document de travail du Comité 29, *op. cit.* (note 11), p. 26.
(30) Lettre (e) de l'art. 26(1).
(31) V. Document de travail du Comité 29, *op. cit.* (note 11), p. 26.
(32) *Ibid.*

pas là d'une exception de caractère général en matière de transferts de données contenues dans les registres publics. En vertu du considérant 58 de la directive, les transferts portant sur la totalité des données ou sur des catégories de données figurant dans ce registre ne sont pas couverts par cette dérogation. Le Comité 29 a relevé, à titre d'exemple, que les transferts massifs, à des fins commerciales, de données contenues dans des registres publics ou la recherche minutieuse de données, accessibles au public, dans le but de dresser le profil de certaines personnes, n'étaient pas couverts par la dérogation (33). Cette dérogation viserait en fait à permettre à la personne qui aurait le droit de consulter un registre public si elle se trouvait sur le territoire de l'Etat membre concerné, de se faire transmettre les informations demandées, nonobstant le fait qu'elle se trouve en réalité dans un pays tiers et que la consultation implique un transfert de données (34).

II. – LE SYSTÈME DU *SAFE HARBOR*

12. Outre-Atlantique, l'adoption de la directive et plus particulièrement son article 25, ont suscité une certaine émotion, puisqu'à moins de tomber dans l'une des dérogations strictement définies de l'article 26, le transfert de données à caractère personnel vers les Etats-Unis risquait d'être purement et simplement interdit (35). En outre, l'alternative consistant à opérer les transferts de données personnelles en violation des dispositions nationales de transposition de la directive, n'était guère réjouissante pour les entreprises américaines, puisqu'elle les faisait encourir des sanctions non seulement civiles, mais aussi pénales, pouvant aller dans certains cas jusqu'à l'emprisonnement.

Ainsi, sans attendre l'adoption, alors encore probablement hypothétique et aléatoire de clauses contractuelles types par la Commission (36), les Etats-Unis se sont efforcés de développer un système original de protection des données qui pourrait être reconnu comme garantissant une protection adéquate au sens de la directive.

Le système du *Safe Harbor* représente le fruit de deux années de négociations entre les Etats-Unis et l'Union européenne. Dès le mois de novembre 1998, soit un mois après l'entrée en vigueur de la directive, les Etats-Unis, par le biais du ministère du Commerce américain, avaient publié un premier texte intitulé *Elements of effective self-regulation for privacy protection.* Les discussions avec la Commission européenne s'étaient poursuivies sur cette base. Le système actuel du *Safe Harbor* reste d'ailleurs très largement inspiré de ce document, même s'il y apporte certaines modifications non négligeables, notamment en ce qui concerne son effectivité (37).

(33) *Ibid.*
(34) *Ibid.* V. également Cullen International, *op. cit.* (note 26), p. 102.
(35) V. H. Heil, Safe Harbor : ein Zwischenstandbericht, Datenschutz und Datensicherheit 24 janv. 2000, p. 444. V. également, F. Deschamps, Microsoft décide d'adhérer aux *Safe Harbor Principles,* 28 mai 2001, p. 2 (<http ://www.droit-technologie.org>).
(36) V. *infra,* n° 29 et s.
(37) V. Y. Poullet, *op. cit.* (note 16), p. 6.

Le système du *Safe Habor* a été adopté par le département du Commerce américain le 21 juillet 2000 et approuvé par la décision de la Commission du 26 juillet 2000 (ci-après « décision de la Commission »), nonobstant l'opposition du Parlement européen (38). L'article 1er de cette décision établit que doivent être réputés garantir un *niveau adéquat de protection* au sens de l'article 25 de la directive *(supra,* n° 4) les transferts de données personnelles depuis l'Union européenne vers des organisations établies aux Etats-Unis qui ont lieu dans les conditions prévues par le système du *Safe Harbor.* Ces conditions ressortent d'un ensemble assez complexe de documents qui comprennent notamment : 1°) une liste de sept principes figurant à l'annexe I de la décision ; 2°) une série de quinze « questions fréquemment posées » *(Frequently Asked Questions,* ci-après « FAQ ») figurant à l'annexe II et destinées à préciser la portée des principes dans la pratique ; et 3°) des échanges de courriers entre le ministère américain du Commerce, la *Federal Trade Commission* (ci-après « FTC ») et la Commission européenne. L'interprétation et le respect de ce système sont soumis au droit américain (39).

On commencera par décrire le mode d'adhésion au *Safe Harbor* (A), pour examiner ensuite les obligations des entreprises américaines adhérentes (B) ainsi que les sanctions du non-respect de ces obligations (C).

A. — *Mode d'adhésion au* Safe Harbor

13. La principale caractéristique du système de *Safe Harbor* réside dans le fait qu'il repose sur une logique non point législative mais plutôt d'autorégulation (40). Ainsi, l'adhésion au système du *Safe Harbor* s'effectue sur une base volontaire. Elle est exclusivement ouverte aux entreprises américaines recevant des données à caractère personnel en provenance de l'Union européenne et relevant de la compétence, soit de la FTC sur la base de la section S

(38) Cette opposition s'est officialisée à travers la résolution du Parlement du 5 juillet 2000 (*supra,* note 14). Les membres du Parlement avaient estimé que le système devait comporter davantage de garanties, dont notamment la reconnaissance du droit de tout individu à introduire une plainte devant un organisme public indépendant, et que dès lors le texte de l'accord devait être renégocié. Dans cette résolution, le Parlement attirait également l'attention de la Commission sur le risque que l'échange de lettres entre la Commission et le ministère américain du Commerce au sujet de la mise en œuvre du *Safe Harbor puisse être interprété par les autorités judiciaires européennes et/ou américaines comme ayant la substance d'un accord international qui aurait été adopté en violation de l'article 300 du Traité CE et de l'obligation de demander l'avis* Commission devant la Cour de justice européenne, sur base du fait que la Commission aurait manqué à ses obligations découlant de la directive, notamment en omettant d'élaborer, avant l'entrée en vigueur de la directive, des clauses contractuelles standardisées, que les citoyens européens pourraient invoquer devant les tribunaux des pays tiers. Le Parlement avait accordé à la Commission jusqu'au 30 septembre 2000 pour soumettre son projet de clauses contractuelles. Ces clauses ont finalement été adoptées le 15 juin 2001 : V. *infra,* n° 29 et s.

(39) V. décis. de la Commission, annexe I (citée *supra,* note 5), p. 6.

(40) En réalité, comme l'a souligné Yves Poullet, le fait que le *Safe Harbor* allie les vertus de l'autoréglementation et de l'autorité de la puissance publique, semblerait plutôt indiquer qu'il s'agit d'un *effective mix* selon la qualification récemment utilisée lors des débats de l'OCDE. En effet, il s'avère que, non seulement le ministère du Commerce américain est à l'origine de ce système, mais qu'aussi, comme nous le verrons ci-après, des organes juridictionnels sont chargés de veiller à son effectivité. V. Y. Poullet, *op. cit.* (note 16), p. 3.

du *Federal Trade Commission Act,* soit du ministère des Transports américain. Il y a lieu de relever que sont en conséquence actuellement exclues les entreprises relevant des secteurs des télécommunications et financier. En ce qui concerne ce dernier secteur, on relèvera que l'entrée en vigueur aux Etats-Unis, le 12 novembre 1999, de la loi *Gramm-Leach-Bliley* (41) limitant la divulgation, par les établissements financiers, d'informations à caractère personnel relatives à leurs clients et autorisant la FTC, les autorités bancaires fédérales et d'autres autorités à adopter des dispositions en vue de la mise en œuvre des mesures prescrites de protection de la vie privée (42), devrait tendre à promouvoir son intégration au sein du *Safe Harbor.*

14. L'engagement d'adhésion au *Safe Harbor* peut revêtir la forme d'une lettre d'autocertification signée d'un cadre de l'entreprise concernée et remise au ministère américain du Commerce (ou à la personne désignée par celui-ci) (43), mais il peut également s'effectuer par l'intermédiaire du formulaire d'inscription informatique disponible sur le site internet du ministère (44). Il vaut pour une période de 12 mois, à l'issue de laquelle l'entreprise américaine devra envoyer une nouvelle lettre, ou formulaire d'autocertification, à défaut de quoi elle se verra rayée de la liste et ne pourra plus bénéficier des avantages du *Safe Harbor* (45). La liste des entreprises ou organisations adhérentes au *Safe Harbor* (46) est publique, elle peut notamment être consultée sur le site du ministère américain du Commerce (47).

L'engagement d'adhésion contient un certain nombre d'informations relatives à l'entreprise adhérente, qui comprennent notamment son nom, ses coordonnées, une description de ses activités relatives aux informations à caractère personnel en provenance de l'Union européenne, une explication du dispositif de protection des données personnelles mis en place, sa date de mise en œuvre, le service de contact en cas de plaintes, le nom de l'instance réglementaire spécifique compétente pour statuer sur les plaintes introduites, la méthode de vérification, et l'instance de recours indépendante chargée d'instruire les plaintes non résolues. L'engagement doit stipuler expressément que l'entreprise américaine respectera les principes du *Safe Harbor,* à compter de son adhésion (48).

L'obligation de respecter les principes du *Safe Harbor* ne vaut pas pour l'ensemble des données à caractère personnel, mais uniquement pour celles re-

(41) L. 106-102, codifiée sous 15 USC, § 6801 et s.

(42) V. décis. de la Commission du 26 juillet 2000 (*supra,* note 5), Annexe III (6).

(43) V. FAQ (*supra,* note 5) n° 6, décis. de la Commission du 26 juill. 2000, annexe II.

(44) Le formulaire est disponible à l'adresse suivante : <http ://web.ita.doc.gov/safeharbor/shreg.nsf/safeharbor?openform>.

(45) *Ibid.*

(46) Connues également en anglais sous le nom de *harborites.* V. not., le document de la Commission intitulé : How will the « safe harbor » arrangement for personal data transfers to the US work ?, <http ://www.europa.eu.int/comm internal_market/en/dataprot/news/datatransf.htm>.

(47) A l'adresse internet suivante : <http ://web.ita.doc.gov/safeharbor/shlist.nsf/webPages/safe%20harbor%20list!OpenDocumet&Star=1>. Il convient ici de relever qu'à tout moment, l'entreprise adhérente peut décider de se retirer du *Safe Harbor,* en notifiant sa décision au ministère du Commerce. Le retrait de la liste met fin à la représentation d'adhésion aux règles du *Safe Harbor,* mais ne libère pas l'entreprise des obligations auxquelles elle s'est engagée à l'égard des informations personnelles qu'elle a reçues du temps de son adhésion (V. *infra* ce numéro).

(48) V. FAQ (*supra,* note 43) n° 6.

ques *au départ de l'Europe* après l'adhésion de l'entreprise en question. En pratique, cette règle a pour effet d'assujettir les données en provenance de l'Europe à un régime différent de celui habituellement suivi pour le reste des données (49). En outre, l'engagement signifie que l'entreprise continuera à appliquer la protection garantie par le *Safe Harbor* aux données reçues en provenance de l'Europe au cours de la période durant laquelle l'entreprise faisait partie du *Safe Harbor,* aussi longtemps qu'elle stockera, utilisera ou divulguera celles-ci, et même dans l'hypothèse où l'entreprise viendrait à quitter ultérieurement pour quelque motif que ce soit le *Safe Harbor* (50). Certains auteurs n'ont pas manqué de relever que cette règle créait en fait une difficulté supplémentaire pour les entreprises américaines ayant adhéré au *Safe Harbor* et décidé par la suite de ne plus y adhérer : de telles sociétés *devront non seulement traiter les informations américaines et européennes différemment mais devront également se réserver la preuve, pour les données européennes, de la date exacte à laquelle elles les ont reçues,* sans parler du problème lié au cas où l'entreprise *recevrait des données à caractère personnel concernant un consommateur européen, pendant son adhésion et en recevrait d'autres concernant le même consommateur après qu'elle ait mis fin à cette adhésion* (51).

B. — *Obligations des entreprises américaines ayant adhéré au* Safe Harbor

15. En adhérant au *Safe Harbor,* les entreprises américaines souscrivent aux obligations qui ressortent des sept grands principes figurant à l'annexe I de la décision de la Commission ; ces principes seront étudiés tour à tour à la lumière des précisions fournies dans le document « FAQ » de l'annexe 2 de la décision (52).

16. En vertu du principe dit de *notification,* l'entreprise est tenue d'informer, par le biais d'une notification claire et lisible, les personnes concernées avant toute collecte d'informations personnelles (i) des raisons de la collecte et de l'utilisation, (ii) des moyens de la contacter pour toute demande ou plainte, (iii) de l'identité des tiers auxquels elles seront communiquées, et (iv) des choix et des moyens pour limiter l'utilisation et la divulgation de ces données (53).

(49) V. Y. Poullet, *op. cit.* (*supra,* note 16), p. 6. Il semble qu'en pratique un grand nombre d'organisations ne remplissent pas cette exigence. Ainsi, la Commission a relevé que pour certaines organisations : aucune déclaration publique d'adhésion n'avait pu être trouvée, abstraction faite de l'autocertification proprement dite, tandis que pour d'autres il n'avait pas été possible d'accéder à leur politique de protection de vie privée mentionnée dans l'autocertification. Document de travail des services de la Commission sur l'application de la décision 520/2000/CE du 13 févr. 2002, SEC(2002)196, (ci-après « Document de travail de la Commission sur l'application de la décision 520/2000/CE »), p. 8 et 10.

(50) FAQ (*supra,* note 43) n° 6.

(51) S. Huart, *op. cit.* (*supra,* note 1) p. 15.

(52) En pratique, la Commission a cependant relevé, de manière préoccupante, que moins de la moitié des organisations adhérentes au *Safe Harbor* avaient adopté des politiques de protection de la vie privée reflétant véritablement la totalité de ces sept principes. V. Document de travail de la Commission sur l'application de la décision 520/2000/CE, *op. cit.* (*supra,* note 49), p. 9.

(53) V. Décision de la Commission (*supra,* note 5), annexe 1.

17. Selon le principe de *choix,* la personne concernée doit se voir reconnaître un double système d'option, l'un à caractère négatif, l'autre positif. Elle bénéficie tout d'abord d'un *opt out* qui lui permet de s'opposer à ce que des données à caractère personnel la concernant soient divulguées à un tiers ou puissent être utilisées dans un but incompatible avec les objectifs pour lesquels elles ont été initialement collectées (54). Il est notamment prévu que le recours à cette option doit être « facile et peu coûteux » (55). La personne concernée se voit offrir ensuite un *opt in,* en ce sens que les données dites sensibles (concernant par exemple son dossier médical ou son état de santé, sa race, sa religion, sa sexualité ou encore ses affiliations syndicales) ne peuvent être collectées sans son consentement préalable et explicite. Certaines exceptions ont toutefois été prévues par le *Safe Harbor,* en vertu desquelles même lorsqu'il s'agit de données sensibles, le consentement préalable et explicite de la personne concernée n'est pas requis (56). Ces hypothèses rappellent en partie mais ne correspondent pas exactement à celles prévues à l'article 26 de la directive et examinées plus haut (57). Par exemple, tandis que la directive vise de manière spécifique l'hypothèse où le transfert s'avère nécessaire à la sauvegarde de l'intérêt vital de la personne concernée, le *Safe Harbor* prévoit pareille exception également dans le cas où l'intérêt vital « d'une autre personne » que la personne concernée est en jeu (58). L'on regrettera le défaut d'uniformité totale sur ce point, qui ne trouve aucune raison objective et risque de susciter des confusions.

18. Le principe intitulé *transfert ultérieur* requiert que l'entreprise désireuse de transférer des informations à un tiers agissant en qualité de mandataire s'assure que ce dernier garantisse un niveau de protection des données personnelles équivalent au sien (59).

19. Conformément au principe de *sécurité,* l'entreprise qui crée, gère, utilise ou diffuse des données personnelles doit protéger son système contre la perte, l'utilisation abusive, la consultation illicite, la divulgation, la modification et la destruction de ces données (60).

20. En vertu du principe *d'intégrité des données,* l'entreprise doit assurer la fiabilité des données personnelles qu'elle traite par rapport à l'utilisation prévue ainsi que leur exactitude, exhaustivité et actualité (61).

(54) Par conséquent, lorsque les données sont utilisées dans le cadre d'une action de marketing direct, la personne concernée pourra exercer son droit de refus à tout moment, sous réserve des délais nécessaires pour que l'organisation puisse tenir compte de ce refus. V. FAQ (*supra,* note 43) n° 12.

(55) V. FAQ (*supra,* note 43) n° 12.

(56) C'est le cas lorsque le traitement s'avère être (i) dans l'intérêt vital de la personne concernée ou d'une autre personne ; (ii) nécessaire à la constatation d'un droit ou d'une défense en justice ; (iii) nécessaire pour dispenser des soins médicaux à des fins de diagnostic ; (iv) effectué dans le cadre d'activités légitimes d'une organisation à but non lucratif ; (v) nécessaire au respect par l'entreprise de ses obligations découlant du droit du travail ; et enfin (vi) lié à des données manifestement rendues publiques par l'individu. V. FAQ n° 1.

(57) V. *supra,* n° 6 à 11.

(58) *Supra,* n° 10.

(59) V. Décision de la Commission (*supra* note 5) annexe 1.

(60) V. Décision de la Commission (*supra* note 5) annexe 1.

(61) V. Décision de la Commission (*supra,* note 5) annexe 1.

21. Le principe *d'accès* veut que l'entreprise soit tenue d'offrir aux personnes dont elle détient les données personnelles la possibilité de consulter celles-ci de sorte que ces personnes soient à même de les corriger ou de les supprimer en cas d'inexactitude (62). Ce principe souffre toutefois un certain nombre d'exceptions dont certaines vont d'ailleurs bien au-delà des exceptions prévues par la directive européenne. Ainsi, il apparaît que les entreprises peuvent refuser ou limiter l'accès, en cas de risque de divulgation d'informations commerciales confidentielles, ou encore dans les circonstances où l'accès impliquerait une charge ou des coûts disproportionnés (63). A la lecture de telles exceptions, l'accès apparaît représenter un simple *intérêt* de la personne concernée qui doit être *mis en balance* avec les intérêts de l'entreprise qui détient les données (64), plutôt que comme un véritable droit de la personne concernée.

22. Enfin, selon le dernier principe dit de *mise en œuvre,* l'entreprise adhérente a le choix entre deux méthodes distinctes alternatives pour attester de son respect des principes du *Safe Harbor,* à savoir l'autoévaluation, ou un contrôle extérieur de la conformité (65). Ceci n'empêche pas l'entreprise de choisir d'appliquer cumulativement les deux procédures de contrôle (66).

Dans le cadre de l'autoévaluation, l'entreprise adhérente doit effectuer une déclaration accessible aux personnes concernées, et ce au minimum une fois par an. Cette déclaration vise à informer les personnes de l'existence de mécanismes internes de traitement des réclamations et de systèmes indépendants compétents pour examiner leurs plaintes. Elle doit également organiser des procédures de formation de ses employés avec des sanctions suffisamment dissuasives à la clef en cas de non-respect pour les contrevenants. Aussi, l'entreprise doit justifier de procédures internes de contrôle régulières et objectives. Cette déclaration devra être produite, le cas échéant, dans le cadre d'une enquête ou réclamation pour non-conformité de l'autocertification d'adhésion au *Safe Harbor.* L'entreprise est en outre tenue d'archiver ses pratiques de mise en œuvre du respect du *Safe Harbor* (67).

23. Le contrôle extérieur de la conformité, quant à lui, repose sur des mécanismes divers permettant d'assurer le respect par l'entreprise du *Safe Harbor,* tels que l'audit, la vérification ponctuelle ou l'utilisation d'outils technologiques. Une déclaration attestant qu'un tel contrôle a bien été effectué devra être établie au moins une fois par an par le contrôleur ou l'entreprise adhérente et doit être accessible aux personnes concernées, ou en cas de plainte (68).

On observera que des mécanismes de résolution des litiges ont été développés par des organisations telles *BBBOnline, TRUSTe, AICPA Web Trust* et la *Direct*

(62) V. Décision de la Commission (*supra,* note 5) annexe 1.
(63) V. FAQ (*supra,* note 43) n° 8.
(64) V. Y. Poullet, *op. cit.* (*supra,* note 16), p. 11.
(65) V. FAQ (*supra,* note 43) n° 7.
(66) C'est l'option choisie par Microsoft tel qu'il en ressort du document relatif à son adhésion disponible sur le site internet du ministère du Commerce américain.
(67) V. FAQ (*supra,* note 43) n° 7.
(68) *Ibid.*

Marketing Association (69), mais d'autres méthodes comme l'arbitrage ou la médiation extérieurs peuvent également être utilisées pour autant qu'elles garantissent le respect du principe de mise en œuvre (70).

24. En outre, l'entreprise américaine adhérente peut choisir de s'engager, toujours sur une base volontaire, à coopérer avec les autorités de l'Union européenne chargées de la protection des données, dans le cadre notamment d'une procédure de règlement des plaintes relatives au *Safe Harbor.* Selon cette procédure, qui sera ouverte au cours d'une période de trois ans, les autorités de l'Union, consultées par l'intermédiaire d'un panel informel établi au niveau européen, s'efforceront de donner un avis dans les soixante jours à compter de la réception de la plainte de l'individu ou du recours formé par l'entreprise ; cet avis pourra être rendu public lorsque le panel l'estimera approprié (71). L'entreprise optant pour ce mode de règlement des litiges devra verser une cotisation annuelle n'excédant pas 500 dollars (72). Elle sera tenue de se conformer à l'avis émis par le panel dans un délai de 25 jours à compter de sa notification (73), sous peine de voir l'affaire portée devant la FTC ou toute autre juridiction compétente et de se rendre coupable de violation de la section 5 du *Federal Trade Commission Act* (74).

C. — *Les sanctions en cas de violation du* Safe Harbor *par l'entreprise adhérente*

25. L'adhésion au *Safe Harbor* et la déclaration de respect des principes de protection de vie privée qu'elle implique, expose l'entreprise adhérente à des obligations et une responsabilité qui autrement n'existeraient pas en droit américain. En effet, dès lors que l'entreprise manquera au respect de sa déclaration publique de respect du *Safe Harbor,* l'entreprise se rendra coupable de violation de la section 5 du *Federal Trade Commission Act,* en vertu de laquelle les actions ou pratiques déloyales ou frauduleuses dans le commerce sont prohibées (75).

Les sanctions en cas de violation du *Safe Harbor* par l'entreprise adhérente peuvent aller selon les circonstances, de la publication des violations et l'obli-

(69) Au 7 décembre 2001, 54 des 129 harborites avaient opté pour de tels mécanismes. V. Document de travail de la Commission sur l'application de la décision 520/2000/CE, *op. cit.* (*supra,* note 49), p. 7.
(70) V. Safe Harbor Workbook, publié par le ministère américain du Commerce, <http ://www.export.gov/safeharbor/SafeHarborWorkbook.htm>.
(71) V. FAQ (*supra,* note 43) n° 5.
(72) Actuellement ce versement s'effectue sur un compte bancaire géré par le *US Council for International Business* (USCIB), organe affilié à la Chambre internationale de commerce. V. Document de travail de la Commission sur l'application de la décision 520/2000/CE, *op. cit.* (*supra,* note 49), p. 6.
(73) Y compris en ce qui concerne les mesures de réparation ou d'indemnisation qui pourraient être formulées au profit de particuliers ayant subi un préjudice en raison du non-respect des principes. V. FAQ (*supra,* note 43) n° 5.
(74) V. FAQ (*supra,* note 43) n° 5. Sur cette section, V. *infra,* n° 25.
(75) USC § 45.

gation d'effacer les données, à la suspension ou au retrait de l'agrément, en passant par l'indemnisation (76).

26. Le dispositif mis en place et destiné à garantir l'effectivité du *Safe Harbor* fonctionne en deux temps. Dans un premier temps, ce sont les autorités indépendantes désignées comme compétentes dans la déclaration de l'entreprise adhérente qui vont instruire les plaintes introduites sur base du *Safe Harbor.* Ce n'est qu'en cas d'échec d'un règlement du litige par ces dernières, que la FTC interviendra. La FTC s'est engagée à traiter en priorité les affaires soumises par les organismes de contrôle indépendants tels que *BBBonline ou TRUSTe,* ainsi que par les Etats membres de l'Union européenne (77). Jusqu'à présent très peu de plaintes ont été déposées (78).

27. Dans l'hypothèse où une entreprise adhérente au *Safe Harbor* ne respecterait pas de manière persistante ses obligations, c'est-à-dire, refuserait de se conformer à une décision définitive prise par un organisme d'autoréglementation ou public qui constate qu'elle viole fréquemment les principes, le ministère du Commerce américain, après un préavis de trente jours, indiquera sur la liste publique qu'il tient à jour l'existence de la notification de non-respect des conditions du *Safe Harbour* (79). En outre, il est précisé que toute organisation demandant à être soumise à l'autorité d'un organisme d'autoréglementation afin de pouvoir bénéficier des avantages du *Safe Harbor devra fournir à cet organisme des informations exhaustives sur son adhésion antérieure aux principes* (80). Il ressort de cette précision qu'une nouvelle adhésion au *Safe Harbor* pourrait être compromise par une exclusion antérieure.

28. On relèvera encore que la participation au *Safe Harbor* ne constitue *pas* une garantie de conformité avec les législations nationales de tous les Etats membres. Certaines législations peuvent en effet aller plus loin dans leurs standards de protection de vie privée que la directive. L'adhésion et le respect du *Safe Harbor* ne met pas les entreprises américaines à l'abri des sanctions qui peuvent les frapper en cas de violation de ces législations. La seule assurance que l'entreprise retire de sa participation fidèle au *Safe Harbor,* est qu'elle ne verra pas, *a priori, ses* transferts de données au départ de l'Europe vers les Etats-Unis interrompus.

29. Un document de travail relatif à l'application du système du *Safe Harbor* vient d'être publié par la Commission, le 13 février 2002 (81). Dans ce rapport qui répond à l'engagement que le commissaire Bolkenstein avait pris de veiller à

(76) V. FAQ (*supra,* note 43) n° 11.
(77) *Ibid.*
(78) V. Document de travail de la Commission sur l'application de la décision 520/2000/CE, *op. cit.* (*supra,* note 49), p. 7.
(79) *Ibid.*
(80) *Ibid.*
(81) Document de travail de la Commission sur l'application de la décision 520/2000/CE, *op. cit.* (*supra,* note 49).

ce que le fonctionnement du *Safe Harbor* fasse l'objet d'un contrôle suivi (82), les services de la Commission soulignent l'effet de simplification bénéfique que crée le système du *Safe Harbor* en faveur des exportateurs de données à caractère personnel vers les Etats-Unis et le faible nombre de plaintes qui semble avoir été déposé par les particuliers jusqu'à présent (83). La Commission a cependant relevé, de manière préoccupante, qu'un nombre considérable d'organisations adhérentes ne respectent pas les exigences de transparence du *Safe Harbor* et que les mécanismes de résolution des litiges n'ont non seulement pas fait connaître publiquement leur intention de mettre en œuvre les règles du *Safe Harbor,* mais encore n'ont pas tous adoptés pour eux-mêmes des pratiques conformes au *Safe Harbor* (84). Selon la Commission, il semblerait qu'une partie du moins des insuffisances observées puisse être imputée à des problèmes de rodage du système et que le *Safe Harbor* reste « une option attrayante » pour les organisations pratiquant régulièrement des transferts de données (85). Une augmentation du nombre d'adhérents est d'ailleurs anticipée (86).

III. – LE SYSTÈME DES CLAUSES CONTRACTUELLES TYPES

30. L'adhésion au *Safe Harbor* n'est pas la seule option pour les entreprises ayant l'intention de transférer des données personnelles à destination des Etats-Unis. Selon le paragraphe 2 de l'article 26 de la directive, les Etats membres peuvent autoriser le transfert de données personnelles vers un pays tiers n'assurant pas un niveau de protection adéquat selon les standards de la directive, lorsque le responsable du traitement offre des *garanties suffisantes,* lesquelles peuvent notamment résulter de *Clauses contractuelles appropriées.*

En outre, le paragraphe 4 de la même disposition prévoit la possibilité pour la Commission d'adopter des *Clauses contractuelles types,* auquel cas les Etats membres sont tenus de prendre les mesures nécessaires pour se conformer à la directive.

31. Le 15 juin 2001, la Commission européenne a adopté une décision arrêtant des clauses contractuelles types considérées comme offrant des garanties suffisantes en matière de protection de la vie privée et des droits fondamentaux et des libertés des individus pour le transfert des données à caractère personnel à l'extérieur de l'Union européenne (ci-après, « la décision du 15 juin 2001 ») (87). L'utilisation de ces clauses est purement volontaire, ces dernières n'étant en effet desti-

(82) Mais qui ne vient nullement se substituer à l'évaluation que la Commission doit réaliser en 2003 en vertu de l'article 4 de la décision de la Commission (*supra* note 5). V. Document de travail de la Commission sur l'application de la décision 520/2000/CE, *op. cit.* (*supra,* note 49), p. 4.
(83) V. Document de travail de la Commission sur l'application de la décision 520/2000/CE, *op. cit.* (*supra,* note 49), p. 2, 7 et 11.
(84) *Ibid.* p. 2, 3, 10-11.
(85) *Ibid.* p. 3 et 12.
(86) *Ibid.* p. 5.
(87) Décis. C(2001)497 CE, JOCE L 181/19, 4 juill. 2001. Pour un premier aperçu, V. E. Wéry, La CE publie des clauses-types pour les flux de données personnelles vers les pays-tiers, <http ://www.droit-technologie.org>.

nées qu'à offrir aux sociétés un moyen alternatif « simple » pour se conformer à l'obligation d'assurer un niveau de protection adéquat aux données personnelles transférées de la Communauté vers le reste du monde (88). La Commission a d'ailleurs souligné que sa décision ne devait pas affecter les autorisations nationales que les Etats membres peuvent délivrer conformément aux dispositions nationales mettant en œuvre l'article 26, § 2, de la directive (89). La Commission a en outre confirmé qu'elle examinerait à l'avenir les clauses contractuelles types présentées par des organisations commerciales ou d'autres parties concernées afin de déterminer si elles offrent des garanties suffisantes conformément à l'article 26, § 2, de la directive (90). Ainsi, les préoccupations qui avaient été émises par ceux qui craignaient que l'adoption des clauses contractuelles types ne soit perçue comme l'imposition *de facto* d'un standard aux entreprises semblent avoir été entendues (91).

32. En vertu de la décision du 15 juin 2001, à compter du 3 septembre 2001, les Etats membres se voient dans l'obligation de reconnaître que les sociétés utilisant les Clauses contractuelles types assurent un *niveau de protection adéquat* et respectent les exigences de la directive afférentes au transfert des données vers des pays tiers qui n'assurent pas un niveau de protection adéquat des données à caractère personnel (92).

Les autorités de contrôle des Etats membres conservent toutefois la faculté d'interdire ou de suspendre un transfert de données ou un ensemble de transferts sur base des Clauses contractuelles types dans trois types de circonstances exceptionnelles qui visent les cas où : 1°) l'importateur est contraint en vertu du droit auquel il est soumis de déroger aux règles pertinentes de protection des données ; 2°) l'importateur n'a pas respecté les clauses du contrat ; 3°) il existe une grande probabilité que les clauses ne sont ou ne seront pas respectées en pratique (93).

Cette faculté des Etats membres de ne pas reconnaître le caractère de *niveau de protection adéquat* aux transferts basées sur des clauses contractuelles types se veut doublement encadrée. Tout d'abord, l'interdiction ou la suspension se doit d'être levée dès que les raisons qui la motivaient disparaissent. Ensuite, les Etats membres sont tenus d'informer sans délai la Commission de toute décision d'interdiction ou de suspension de flux de données (94).

33. Les Clauses contractuelles types n'ayant trait qu'à la protection des données *à caractère personnel*, les importateurs et exportateurs de données qui décident d'en faire utilisation, restent libres d'inclure les autres clauses à caractère commercial qu'ils jugeraient pertinentes pour leurs contrats sous réserve, toutefois, qu'elles ne contredisent pas les Clauses contractuelles types (95).

(88) V. le document de la Commission intitulé : Protection des données : la Commission approuve des clauses contractuelles types pour les transferts de données vers des pays tiers, <http ://www.europa.eu.int/comm/internal_market/fr/dataprot/news/clauses2.htm>.
(89) V. considérant 6 de la décision du 15 juin 2001.
(90) V. considérant 10 de la décision du 15 juin 2001.
(91) V. notamment les correspondances échangées entre la Commission et les organisations économiques et les ministères américains des Finances et de l'Economie, <http ://www.europa.eu.int/comm/internal_market/en/dataprot/news/clausesexchange.htm>.
(92) *Ibid.*
(93) V. art. 4(1) de la décision du 15 juin 2001.
(94) V. al. 2 et 3 art. 4 de la décision du 15 juin 2001.

34. Parmi les Clauses contractuelles types, l'on retiendra les plus importantes d'un point de vue pratique. Tout d'abord, la Clause 3 dite du *tiers bénéficiaire* qui permet aux personnes concernées par les données personnelles de faire appliquer une grande partie (mais pas la totalité) (96) des clauses contractuelles en tant que tiers bénéficiaires, leur conférant ainsi une protection appréciable. Cette protection est d'autant accrue, que les parties au contrat s'engagent à accepter que les personnes concernées soient éventuellement représentées par une association ou d'autres organismes.

35. Les Clauses contractuelles types contiennent en outre une déclaration juridiquement exécutoire ou *garantie* par laquelle l'importateur de données s'engage à traiter les données personnelles conformément à un ensemble de principes fondamentaux de protection des données (Clauses 4 et 5).

36. La Clause 6 instaure un principe de *responsabilité conjointe et solidaire* de l'exportateur et de l'importateur des données. Destinée principalement à réduire les difficultés d'ordre pratique que les personnes concernées pourraient rencontrer lorsqu'elles tentent de faire appliquer leurs droits en vertu des Clauses contractuelles types (97), elle vise également à encourager les parties à accorder une attention particulière au respect des clauses contractuelles de protection des données par l'autre (98). Cette clause a fait couler beaucoup d'encre, les organisations économiques lui reprochant d'aller directement à l'encontre de la réalité économique (99). C'est vraisemblablement pour répondre à cette critique que la Commission a réduit dans une certaine mesure la portée de la responsabilité conjointe et solidaire. Ainsi, cette responsabilité ne s'applique qu'aux dispositions expressément mentionnées par la Clause 3 dite du tiers bénéficiaire. Elle ne s'étend ainsi plus, comme c'était le cas dans les versions précédentes, à la violation de la totalité des Clauses contractuelles (100). Par ailleurs, une clause facultative de dédommagement mutuel est incluse dans les clauses contractuelles types dans un souci de clarification et pour faciliter la tâche des parties (101). Relevons, enfin, que le concept de responsabilité a été aligné dans la mesure du possible sur celui de l'article 22 de la directive, avec notamment comme conséquence que l'importateur et l'exportateur peuvent être exemptés de toute res-

(95) V. considérant 5 de la décision du 15 juin 2001.
(96) Sont seules applicables les Clauses 4b-c-d, 5a-b-c-e, 6-1° et 6-2°, 7, 9 et 11.
(97) V. considérant 18 de la décision du 15 juin 2001.
(98) V. notamment les correspondances échangées entre la Commission et les organisations économiques et les ministères américains des Finances et de l'Economie (*supra,* note 91).
(99) V. notamment les correspondances échangées entre la Commission et les organisations économiques et les ministères américains des Finances et de l'Economie (*supra,* note 91).
(100) V. notamment la réponse adressée par la Commission à la Chambre internationale du commerce parmi les correspondances échangées entre la Commission et les organisations économiques et les ministères américains des Finances et de l'Economie (*supra,* note 91), annexe.
(101) *Ibid.*

ponsabilité s'ils ramènent la preuve que le dommage causé n'est imputable à aucun d'entre eux (102).

37. La Clause 4(c), apparemment anodine, en ce qu'elle oblige simplement l'exportateur de données à mettre à la disposition des personnes concernées, sur leur demande, une *copie des clauses* telles que convenues, a également été sujette à vive controverse. Les organisations économiques estimaient que l'ensemble des informations contenues dans les clauses devait bénéficier d'une présomption de confidentialité. Ainsi, selon elles, le contenu des clauses ne devait être révélé en principe qu'aux autorités de contrôle. A juste titre, la Commission n'a pas retenu cette solution. Le droit d'obtenir la copie des clauses ne paraît en effet pas de nature à porter atteinte à la nécessaire protection des informations confidentielles, puisqu'il va de soi que le droit des personnes concernées d'obtenir une copie des clauses ne concerne que les Clauses contractuelles types ayant trait à la protection des données, et ne s'étend pas aux autres clauses à caractère commercial que l'importateur et l'exportateur de données pourraient décider d'inclure dans leurs contrats.

38. Relevons enfin, qu'en vertu de la Clause 7 qui vise l'hypothèse où un litige opposant la personne concernée à l'exportateur et l'importateur de données ne pourrait être résolu à l'amiable et pour lequel la personne concernée invoquerait la clause du tiers bénéficiaire, ces derniers sont tenus de lui proposer *le choix* entre la médiation, l'arbitrage et le procès. La personne concernée pourra, si elle le souhaite, porter le litige devant les tribunaux de l'Etat membre où l'exportateur de données est établi.

39. La décision de la Commission du 15 juin 2001 n'est qu'un premier pas dans l'élaboration de solutions contractuelles « sur mesure » pour le transfert de données à caractère personnel au niveau mondial. La décision mentionne expressément que son application sera revue à la lumière de l'expérience acquise (103) et la Commission a déjà annoncé son intention d'adopter d'autres décisions en fonction des catégories spécifiques de transferts (104). Ainsi des clauses contractuelles types pour le transfert de données à caractère personnel vers des sous-traitants établis dans des pays tiers viennent d'être adoptées (105). Il reste à voir si ce phénomène accru de reconnaissance de clauses contractuelles types par la Commission ne sonnera pas le glas du système du *Safe Harbor*.

(102) V. Clause 6(1). V. également la réponse adressée par la Commission à la Chambre internationale du commerce parmi les correspondances échangées entre la Commission et les organisations économiques et les ministères américains des Finances et de l'Economie (*supra*, note 91).

(103) V. considérant 9 de la décision du 15 juin 2001.

(104) *Ibid.*

(105) V. la décision de la Commission 2002/16/CE du 27 déc. 2002, JOCE L 6, 10 janv. 2002.

CONCLUSION

40. Les systèmes du *Safe Harbor* et des *Clauses contractuelles types* partagent le même objectif général : celui de concilier les besoins des entreprises de transférer des données à caractère personnel vers des Etats tiers avec la nécessaire protection de la vie privée des personnes concernées par ces données lorsque le transfert a lieu vers un pays dont la réglementation n'assure pas *a priori* un niveau de protection suffisant au regard du droit communautaire. Pourtant, même s'ils ont la même finalité, ces deux systèmes, comme le démontrent les explications qui précèdent, ont un régime juridique assez différent.

Dès lors que chacun des deux systèmes est optionnel et que son application dépend d'une adhésion volontaire de la part des entreprises intéressées, on pourrait s'attendre à ce que l'un des deux systèmes émerge de la pratique comme étant le préféré des décideurs économiques, à savoir celui qui s'avérerait le moins contraignant pour les entreprises concernées.

D'aucuns ont ainsi émis la crainte que l'adoption des Clauses contractuelles types par la Commission entraîne une perte d'intérêt pour le système du *Safe Harbor* (106) qui, avec l'adhésion de Microsoft, aurait en quelque sorte connu le sort d'un feu d'artifice. Il est vrai que les Clauses contractuelles types présentent *a priori* de nombreux avantages par rapport au *Safe Harbor*. Tout d'abord, on relèvera qu'une fois signées, et pour autant que le contrat reste en vigueur et que les parties le respectent, les Clauses présentent le grand avantage pratique de ne plus nécessiter l'accomplissement de nouvelles formalités (107). Par contraste, le *Safe Harbor* requiert qu'un nouveau formulaire d'autocertification soit rempli sur une base annuelle. En outre, les Clauses contractuelles types sont relativement claires et leur portée peut être dégagée en ayant égard en principe uniquement à la décision de la Commission du 15 juin 2001. A l'inverse, le *Safe Harbor* ne bénéficie pas d'une base très structurée : il repose sur un ensemble relativement désorganisé de principes, de « questions fréquemment posées », et de documents divers qui participe en pratique à créer une certaine confusion. Enfin, les Clauses contractuelles types ont potentiellement un champ d'application plus vaste que le *Safe Harbor,* à la fois sur le plan matériel, puisqu'elles ne sont pas limitées à des secteurs particuliers de l'industrie, et sur le plan géographique, dès lors qu'elles ont vocation à s'appliquer à l'échelle mondiale et non uniquement aux données à destination des Etats-Unis.

Pourtant, force est de constater que l'adoption des Clauses contractuelles types n'a pas freiné l'engouement croissant dont bénéficie, en pratique, le système du *Safe Harbor* auquel ont déjà adhéré, au 1er janvier 2002, plus de 150 entreprises américaines. Des raisons substantielles permettent d'expliquer ce phéno-

(106) V. l'avis du gouvernement américain émis lors de la publication du projet de décision relatif aux clauses contractuelles types : « [w]e are concerned future negotiations for the financial services sector may be adversely affected by the Commission's proposal to adopt standard clauses for contracts governing data transfers from firms in the EU to firms in other countries » (Lettre du *Department of Treasury* du 23 mars 2001 à l'attention de John Mogg, *in* Correspondances échangées entre la Commission et les organisations économiques et les ministères américains des Finances et de l'Economie, *supra* note 81). V. aussi S. Huart, *op. cit.* (note 1) p. 16.

(107) V. B. Goodger, Cross-Border Data Transfer : The Safe Harbor and EU Model Clauses Compared, EuroWatch, vol. 13, n° 15, 15 août 2001.

mène : c'est que l'autorégulation sur lequel est fondé le *Safe Harbor* entraîne une plus grande souplesse dans la détermination des obligations qui pèsent sur les entreprises ayant adhéré au système. On relèvera tout d'abord qu'en ce qui concerne le règlement des différends, le *Safe Harbor* se borne à prévoir un système optionnel de recours à des mécanismes de résolution des litiges développés par des organismes indépendants (*supra,* n° 22 et s. et 26), sans conférer un droit de recours individuel à une autorité publique (108). Par contraste, les Clauses contractuelles types offrent nécessairement la possibilité à la personne concernée de porter le litige devant les tribunaux de l'Etat membre où l'exportateur des données est établi (*supra,* n° 36), ce qui risque d'effrayer les entreprises américaines. En outre, le *Safe Harbor* ne prévoit pas que l'entreprise américaine importatrice de donnée sera responsable du respect par l'exportateur des données des obligations qui pèse sur elle concernant ce transfert. Ceci contraste à nouveau avec les Clauses contractuelles type, qui prévoient une responsabilité conjointe et solidaire de l'exportateur et l'importateur des données (*supra,* n° 5). Il s'agit là d'une clause assez redoutable en pratique pour les entreprises américaines qui risquent de voir leur responsabilité mise en cause en raison des irrégularités ou omissions de la part de leur co-contractant européen.

41. Pour conclure, on observera la richesse des moyens juridiques qui sont à présent à la disposition des entreprises qui envisagent de procéder au transfert de données à caractère personnel vers les Etats-Unis conformément à la directive 95/46/CE. La mise en œuvre de ces moyens est relativement flexible et dépend d'une analyse au cas par cas des besoins de chaque entreprise, en fonction des caractéristiques propres des transferts envisagés. C'est une approche pragmatique qui a prévalu dans cette matière extrêmement sensible où doivent se combiner harmonieusement le respect des droits fondamentaux de l'homme et les intérêts économiques.

Janvier 2002

(108) C'est d'ailleurs l'absence d'un tel recours qui a conduit le Parlement européen a considérer que le système du *Safe Harbor* n'assure pas une protection suffisante des personnes concernées par le transfert des données (V. la résolution du Parlement, *supra* note 14, p. 5).

Le principe de précaution : exception à l'application du droit communautaire ?*

Philippe ICARD

Maître de conférences à l'Université de Bourgogne
Directeur du Centre de recherche de droit européen
Membre du Centre de droit public et économique

Le droit communautaire connaît depuis son origine des techniques juridiques permettant, par exception, d'éviter de l'appliquer.
Le principe de précaution entre-t-il dans cette catégorie ? Voilà tout le propos de cet article.
La réponse varie en fonction de l'organe qui le met en œuvre. En effet, lorsqu'il intervient par la volonté des instances communautaires, il s'agit d'une dérogation. En revanche, revendiqué par un Etat membre, sa qualification juridique change pour devenir une exception.

L'engouement suscité par le principe de précaution est à la hauteur des difficultés juridiques qu'il engendre. Jusqu'à présent, le lien entre le droit et la science fut toujours marqué du sceau de la certitude. Le droit communautaire n'échappait pas à cette constatation. En effet, l'utilisation de l'article 30 CE (1) par les Etats membres, afin d'empêcher l'application du principe de libre circulation des marchandises, exigeait la démonstration de la réalité du risque pesant sur la santé ou la sécurité.

Or, le principe de précaution reformule le rapport du droit à la science en introduisant le doute (2).

(*) Article issu d'une communication à un colloque relatif à L'exception en droit communautaire, organisé à la Faculté de droit de Clermont-Ferrand, sous la direction de Christine Bertrand et de Florence Stirling-Belin.

(1) Art. 30 : « Les dispositions des articles 28 et 29 ne font pas obstacles aux interdictions ou restrictions d'importations, d'exportation ou de transit, justifiées par des raisons d'ordre public, de sécurité publique, de protection de la santé et de la vie des personnes et des animaux ou de préservation des végétaux (...) ».

(2) V. Laurence Baghestani-Perrey (dir.), La décision publique et le droit de la responsabilité face au principe de précaution, colloque de la faculté de droit de Dijon, n° spéc. RJE déc. 2000 et du même auteur, Le principe de précaution : nouveau principe fondamental régissant les rapports entre le droit et la science, D. 1999, n° 11, p. 457 ; L. Zaccaï et J.-M. Missa (dir.), Signification et conséquences du principe de précaution, Presses de l'Université Libre de Bruxelles, 2000 ; L. Gonzalez-Vaque, L. Ehring et G. Jaquet, Le principe de précaution dans la législation communautaire et nationale relative à la santé, Rev. Marché commun et de l'Union européenne, 1999.79 ; G. Corcelle, La perception communautaire du principe de précaution, Rev. Marché commun et de l'Union européenne, 2001.447 ; Journal des tribunaux, L'émergence du