Aterritorialité des atteintes face aux logiques territoriales de protection juridique et problème de l'absence d'homogénéité des législations protectrices (quid des *safe harbor principles*)

Cynthia Chassigneux

Vie privée et interconnexions : vers un changement de paradigme?
Conférence organisée par le Programme international de coopération scientifique
(CRDP / CECOJI)
Ivry sur Seine, 5 juin 2003

Lex Electronica, vol. 9, n°2, Numéro Spécial, hiver 2004
http://www.lex-electronica.org/articles/v9-2/chassigneux.htm

Introduction

Les affaires *DoubleClick*, *Toysmart*, *Boo.com*, *eBay*, *Amazon*, *Yahoo!* ou, plus récemment, le transfert de données des dossiers passagers par les compagnies aériennes ravivent le débat quant à l'encadrement juridique des renseignements personnels dans un environnement électronique. Ces problématiques concernent aussi bien le secteur public que privé, soit l'ensemble des branches du droit. Elles doivent de plus s'envisager à une échelle non plus nationale mais internationale eu égard à la « mondialisation » des communications et des échanges ... et des atteintes susceptibles d'être portées aux renseignements personnels.

Pour s'en rendre compte, il suffit de se rappeler l'affaire *DoubleClick* relative, d'une part, à l'utilisation de bannières publicitaires affichées sur les pages des sites affiliés à la régie pour profiler les habitudes de consommation et de navigation des internautes, quelle que soit leur nationalité, à leur insu et, d'autre part, à l'interconnexion des fichiers de la régie avec ceux de la société de *marketing* direct *AbacusDirect*[1]. Il est également possible de se référer à la communication, par les compagnies aériennes, des renseignements personnels de tous les passagers et membres d'équipage aux autorités américaines, canadiennes et australiennes à des fins de sécurité nationale[2].

Cette « soif de connaissance » des entreprises privées et des autorités publiques inquiète, surtout en ce qui concerne le traitement des données après leur collecte, l'information des personnes concernées, ou encore l'accès et le droit de rectification devant leur être reconnu. Cette préoccupation est d'autant plus forte qu'il n'existe pas une mais plusieurs conceptions de la protection à accorder aux renseignements personnels. Dès lors, comment une personne physique peut-elle faire valoir ses droits à l'égard d'un pays qui n'offre pas les mêmes garanties en la matière ? Sur quelle base une personne morale doit-elle négocier le transfert de renseignements personnels vers un pays tiers à son système juridique ?

---

[1] Au sujet de l'affaire *DoubleClick*, il est possible de consulter, entre autres, ELECTRONIC PRIVACY INFORMATION CENTER, « EPIC Files FTC Complaint Against DoubleClick, Alleges « Deceptive and Unfair Trade Practice » in Online Data Collection », 10 février 2000, http://www.epic.org/privacy/internet/ftc/DCLK_comp_pr.html; JUNKBUSTER, « DoubleClick, Abacus Direct and Privacy », http://www.junkbusters.com/doubleclick.html; THE SUPERIOR COURT OF THE STATE OF CALIFORNIA, Harriett Judnick v. DoubleClick Inc., Case No 000421, http://www.arentfox.com/additionalsites/e-privacy/e-privacynews/privacy2000/Judnick.pdf; FEDERAL TRADE COMMISSION, « Letter », 22 janvier 2001, http://www.ftc.gov/os/closings/staff/doubleclick.pdf; In re DoubleClick Inc. Privacy Litigation (Objection by Settlement Class Members), 00-CIV-0641 (NRB) (U.S. District Court for the Southern District of New York), http://www.epic.org/privacy/cookies/doubleclickobjection.pdf; In re DoubleClick Inc. Privacy Litigation, 00-CIV-0641 (NRB) (U.S. District Court for the Southern District of New York), http://www.nysd.uscourts.gov/courtweb/pdf/D02NYSC/01-03797.pdf.

[2] À ce sujet, il est possible de consulter, entre autres, ARTICLE 29 GROUPE DE PROTECTION DES DONNÉES, « Avis 1/2004 sur le niveau de protection assuré en Australie à la transmission de données des dossiers passagers par les compagnies aériennes », WP 85, 16 janvier 2004, http://europe.eu.int/comm/internal_market/privacy/docs/wpdocs/2004/wp85_fr.pdf; « Avis 2/2004 sur le niveau de protection adéquat des données à caractère personnel contenues dans les dossiers des passagers aériens (PNR) transférés au Bureau des douanes et de la protection des frontières des Etats-Unis (US CBP) », WP 87, 29 janvier 2004, http://europe.eu.int/comm/internal_market/privacy/docs/wpdocs/2004/wp87_fr.pdf; « Avis 3/2004 sur le niveau de protection assuré au Canada à la transmission, par les compagnies aériennes, des dossiers passagers et d'informations anticipés sur les voyageurs », WP 88, 22 février 2004, http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2004/wp88_fr.pdf.

Ces questions s'illustrent particulièrement au regard de la *Directive 95/46/CE du Parlement européen et du Conseil 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*[3]. Cette directive vise à concilier la protection des données à caractère personnel avec la libre circulation de celles-ci non seulement au sein de l'Union européenne, mais aussi en direction de pays tiers, comme en dispose l'article 25 paragraphe 1,

> *1. Les États membres prévoient que le transfert vers un pays tiers de données à caractère personnel faisant l'objet d'un traitement, ou destinées à faire l'objet d'un traitement après leur transfert, ne peut avoir lieu que si, sous réserves du respect des dispositions nationales prises en application des autres dispositions de la présente directive, le pays tiers en question assure un niveau de protection adéquat.*[4]

Cette exigence[5] a donné lieu à de nombreuses discussions entre l'Union européenne et les États-Unis, ces derniers n'offrant une protection que dans certains secteurs d'activités, les autres s'autorégulant. Dès lors, les discussions ont porté sur les *Safe Harbor Principles* adoptés par le *U.S. Department of Commerce*[6] et acceptés, en juillet 2000, par la Commission européenne[7], soit deux ans après le début des négociations[8].

Si l'accord intervenu entre l'Union européenne et les États-Unis est celui qui a le plus marqué les esprits, il ne faut pas pour autant en oublier les autres décisions de la Commission européenne quant au niveau de protection offert par la Suisse[9], la Hongrie[10], le Canada[11], l'Argentine[12],

---

3 J. O. des Communautés européennes n° L 281 du 23 octobre 1995 p. 0031-0050 (ci-après « Directive 95/46/CE »).

4 Nos soulignements.

5 Il convient de noter qu'une telle exigence est également exprimée, d'une part, dans les *Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel* émises par l'Organisation de Coopération et de Développement Économiques en septembre 1980 (ci-après « Lignes directrices de l'OCDE ») et, d'autre part, dans la *Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel* adoptée par le Conseil de l'Europe en janvier 1981 (ci-après « Convention 108 »).

6 « International Safe Harbor Privacy Principles », 19 avril 1999, http://www.ita.doc.gov/td/ecom/shprin.html. On retrouve déjà ces principes dans une lettre du 4 novembre 1998 émise par David A. Aaron à l'intention du secteur privé, http://www.ita.doc.gov/td/ecom/aaron114.html.

7 *Décision de la Commission du 26 juillet 2000 conformément à la directive 95/45/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*, J.O. des Communautés européennes n° L 215 du 25 août 2000 p. 0007-0047, (ci-après « Décision du 26 juillet 2000 »).

8 Pour une approche chronologique des documents ayant conduit à la décision du 26 juillet 2000, voir notamment http://www.export.gov/safeharbor/sh_historicaldocuments.html.

9 COMMISSION EUROPÉENNE, *Décision de la Commission du 26 juillet 2000 relative à la constatation, conformément à la directive 95/46/CE du Parlement européen et du Conseil, du caractère adéquat de la protection des données à caractère personnel en Suisse*, J.O. des Communautés européennes n° L 215 du 25 août 2000 p. 0001-0003.

10 COMMISSION EUROPÉENNE, *Décision de la Commission du 26 juillet 2000 relative à la constatation, conformément à la directive 95/46/CE du Parlement européen et du Conseil, du caractère adéquat de la protection des données à caractère personnel en Hongrie*, J.O. des Communautés européennes n° L 215 du 25 août 2000 p. 0004-0006.

11 COMMISSION EUROPÉENNE, *Décision de la Commission du 20 décembre 2001 constatant, conformément à la directive 95/46/CE du Parlement européen et du Conseil, le niveau de protection adéquat des*

Guernesey[13] et l'Île de Man[14], ou encore les avis rendus par l'Article 29 Groupe de protection des données concernant le transfert de données des dossiers passagers[15]. Ces décisions et avis ont été rendus en appréciant, tout particulièrement, « la nature des données, la finalité et la durée du ou des traitements envisagés, les pays d'origine et de destination finale, les règles de droit, générales ou sectorielles, en vigueur dans le pays tiers en cause, ainsi que les règles professionnelles et les mesures de sécurité qui y sont respectées. »[16] Pour ce faire, en dehors des dérogations prévues par la *Directive 95/46/CE*[17], il a été nécessaire d'analyser les législations internes ou les engagements internationaux des pays tiers[18]; d'envisager les garanties pouvant « résulter de clauses contractuelles appropriées »[19] ou de codes d'autoréglementation sectoriels[20].

Cette démarche de l'Union européenne s'explique par la volonté de garantir aux personnes physiques, d'une part, un niveau satisfaisant de respect des règles, d'autre part, un soutien et une assistance dans l'exercice de leurs droits et, enfin, des voies de recours appropriées en cas de non-respect des règles[21]. Cette démarche s'explique aussi, selon Louise Cadoux, par le fait que « la mondialisation fait que la protection de la vie privée et des libertés fondamentales ne peut plus être une matière divisible en suivant les contours des aires géographiques ou des États. »[22] De plus, il est rappelé par la Commission européenne que de telles analyses quant à l'adéquation du niveau de protection, compte tenu des différentes approches en la matière, ne doivent pas créer de discriminations arbitraires ou injustifiées à l'égard de pays tiers où des conditions similaires existent ou entre les pays tiers, ni constituer un obstacle déguisé au commerce eu

---

données à caractère personnel assuré par la loi canadienne sur la protection des renseignements personnels et les documents électroniques, J.O. des Communautés européennes n° L 2 du 4 janvier 2002 p. 0013-0016.

12 COMMISSION EUROPÉENNE, *Décision de la Commission du 30 juin 2003 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'Argentine*, J.O. des Communautés européennes n° L 168 du 5 juillet 2003.

13 COMMISSION EUROPÉNNE, *Décision de la Commission du 21 novembre 2003 constatant le niveau de protection adéquat des données à caractère personnel à Guernesey*, J.O. des Communautés européenne n° L 308 du 25 novembre 2003 p. 0027-0028.

14 ARTICLE 29 GROUPE DE PROTECTION DES DONNÉES, *Avis 6/2003 relatif au niveau de protection des données à caractère personnel dans l'Île de Man*, WP 82, 21 novembre 2003, http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2003/wp82_fr.pdf.

15 *Supra*, note 2.

16 *Directive 95/46/CE*, article 25 paragraphe 2.

17 *Directive 95/46/CE*, article 26 paragraphe 1. Voir à ce sujet, entre autres, ARTICLE 29 GROUPE DE PROTECTION DES DONNÉES, *Document de travail : Transfert des données personnelles vers des pays tiers : application des articles 25 et 26 de la directive relative à la protection des données*, WP 12, 24 juillet 1998, http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/1998/wp12_fr.pdf, pp. 25 et suiv.

18 *Directive 95/46/CE*, article 25 paragraphe 6.

19 *Directive 95/46/CE*, article 26 paragraphe 2. Voir à ce sujet, entre autres, ARTICLE 29 GROUPE DE PROTECTION DES DONNÉES, *Document de travail : Vues préliminaires sur le recours à des dispositions contractuelles dans le cadre de transferts de données à caractère personnel vers des pays tiers*, WP 9, 22 avril 1998, http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/1998/wp9_fr.pdf; WP 12, *op. cit.* note 17, pp. 16 et suiv.

20 *Directive 95/46/CE*, article 25 paragraphe 2. Voir à ce sujet, entre autres, ARTICLE 29 GROUPE DE PROTECTION DES DONNÉES, *Document de travail : Évaluation des codes d'autoréglementation sectoriels : quand peut-on dire qu'ils contribuent utilement à la protection des données dans un pays tiers?*, WP 7, 14 janvier 1998, http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/1998/wp7_fr.pdf; WP 12, *id.*, pp. 11 et suiv.

21 ARTICLE 29 GROUPE DE PROTECTION DES DONNÉES, WP 12, *id.*, p. 8.

22 Louise CADOUX, « La protection des données personnelles en dehors de l'Europe communautaire », dans *Revue française d'administration publique*, n° 89, janvier-mars 1999, pp. 83 à 94, à la page 83.

égard aux engagements internationaux actuels de la Communauté[23]. Partant de là, il convient de s'interroger sur la portée de ces décisions et avis, notamment au regard des *Safe Harbor Principles* ou principes de la « sphère de sécurité », une fois le contenu de ces derniers rappelé.

I. Rappel du contenu des *Safe Harbor Principles*

Au regard des avis rendus en janvier 1999 et en mai 2000, force est de constater « que des progrès importants et significatifs visant l'amélioration de la protection des données à caractère personnel ont été réalisés au cours des deux dernières années de négociation avec le ministère américain du commerce et […] les dernières modifications apportées aux principes et aux documents connexes intègrent plusieurs suggestions émises par le groupe de travail dans ses avis précédents. »[24] Ces progrès ont conduit à la reconnaissance des *Safe Harbor Principles*, alors qu'au début des négociations le groupe de travail établi en vertu de l'article 29 de la *Directive 95/46/CE* estimait que l'on ne pouvait pas compter sur un « ensemble disparate, constitué de lois sectorielles très ciblées et de l'autorégulation volontaire pour assurer dans tous les cas une protection adéquate en ce qui concerne les données à caractère personnel transférées à partir de l'Union européenne. »[25]

La reconnaissance du niveau de protection adéquat tient compte non seulement des principes de la « sphère de sécurité » eux-mêmes, mais aussi des questions souvent posées (ou « FAQ ») contenant des orientations quant à la mise en œuvre des principes, étant entendu que ces derniers constituent un minimum devant être respecté par les entreprises et organisations américaines lors du transfert de renseignements personnels venant de l'Union européenne. Cette idée de minimum fait référence à la philosophie ayant conduit l'Organisation de Coopération et de Développement Économiques et le Conseil de l'Europe à adopter respectivement les *Lignes directrices de l'OCDE* et la *Convention 108.*

Ces textes sont, en effet, le fruit d'un dialogue entre pays membres d'une même institution intergouvernementale et constituent des normes minimales en deçà desquelles les pays membres ne peuvent pas légiférer quant à la protection des droits des personnes physiques dont les renseignements personnels font l'objet d'un traitement national et/ou international.

Ainsi, au regard de ceux énoncés dans les *Lignes directrices de l'OCDE*, dans la *Convention 108* et dans la *Directive 95/46/CE* , la « sphère de sécurité » repose sur plusieurs principes visant à encadrer le traitement des renseignements personnels.

---

[23] Une telle considération est rappelée dans chacune des décisions prises par la Commission européenne relative au niveau de protection offert par les pays tiers : Suisse, Hongrie, Canada, Argentine, Guernesey, États-Unis, Île de Man.

[24] ARTICLE 29 GROUPE DE PROTECTION DES DONNÉES, *Avis 4/2000 sur le niveau de protection assuré par les « principes de la sphère de sécurité »*, WP 32, 16 mai 2000, http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2000/wp32fr.pdf, p. 2.

[25] ARTICLE 29 GROUPE DE PROTECTION DES DONNÉES, *Avis 1/99 concernant le niveau de protection des données à caractère personnel aux Etats-Unis et les discussions en cours entre la Commission européenne et le gouvernement américain*, WP 15, 26 janvier 1999, http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/1999/wp15fr.pdf, p. 2.

Notification

Notification
Les personnes concernées doivent être informées : • des raisons de la collecte et de l'utilisation des données; • de la façon de contacter le responsable du traitement pour toute demande ou plainte; • des tiers auxquels les données sont communiquées, et • des choix et des moyens offert pour limiter l'utilisation et la divulgation des données. Elle doit se faire dans un langage clair et lisible. Elle doit se faire au moment la collecte, ou dès que possible, et surtout avant que les données ne soient utilisées dans un but différent de celui pour lequel elles ont été initialement collectées ou traitées par l'organisation ayant effectué le transfert ou avant qu'elles ne soient diffusées pour la première fois à un tiers.
➥ limitation en matière de collecte (*OCDE*); spécification des finalités (*OCDE*); transparence (*OCDE*); qualité des données (*Convention 108 – Directive 95/46/CE*); garanties complémentaires pour la personne concernée (*Convention 108*); information de la personne concernée (*Directive 95/46/CE*)

Par la notification[26], le responsable du traitement informe préalablement, ou dès que possible, la personne concernée des raisons de la collecte et de l'utilisation des renseignements, des tiers qui y auront accès et des droits qui lui sont reconnus. Cette obligation peut s'interpréter de deux manières. D'une part, la notification est synonyme de transparence. Le responsable doit veiller à communiquer, dans des termes compréhensibles, les motifs conduisant à la collecte des renseignements personnels. Cette communication doit être suffisamment accessible pour que la personne concernée puisse facilement en prendre connaissance. Il est donc recommandé de faire figurer cette notification sur la page d'accueil du site Web, idéalement sur toutes les pages et, en particulier sur celles conduisant à la collecte de renseignements personnels.

D'autre part, cette information est nécessaire à l'expression d'un consentement manifeste, libre, éclairé et donné à des fins spécifiques. L'expression d'un tel consentement doit être recherché lorsque le responsable du traitement entend utiliser les renseignements dans un but autre que celui pour lequel les données ont été initialement collectées. Il est, en effet, important que la personne concernée puisse exprimer son consentement, son choix.

[26] Pour une illustration des interrogations soulevées par ce principe, voir notamment : ARTICLE 29 GROUPE DE PROTECTION DES DONNÉES, *Avis 7/99 sur le niveau de protection des données garanti par les principes de la « sphère de sécurité » publiés avec les questions fréquemment posées (FAQ) et d'autres documents connexes les 15 et 16 novembre 1999 par le ministère du commerce américain*, WP 27, 3 décembre 1999, http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/1999/wp27fr.pdf, p. 7.

Choix

Choix
Les personnes concernées doivent avoir la possibilité de décider si leurs données peuvent être : • divulguées à des tiers, ou • utilisées dans un but incompatible avec le ou les objectifs pour lesquels elles ont été initialement collectées ou dans un but approuvé ultérieurement par la personne concernée En ce qui concerne les informations sensibles, les personnes concernées doivent avoir – positivement ou explicitement – la possibilité de décider si leurs données peuvent être : • divulguées à des tiers, ou • utilisées dans un but qui diffère de l'objectif initial de la collecte ou dans un but approuvé ultérieurement par la personne concernée exerçant son droit de consentement.
➥ limitation de l'utilisation (*OCDE*); légitimation des traitements de données (*Directive 95/46/CE*); droit d'opposition (*Directive 95/46/CE*)

La possibilité pour la personne concernée d'exprimer son choix quant à l'utilisation de ses renseignements personnels a fait l'objet de nombreuses discussions[27] au regard, d'une part, du processus de l'*opt-in* et, d'autre part, de celui de l'*opt-out*. Si le premier cas signifie que la personne concernée peut s'opposer au moment de la collecte à l'utilisation de ses données à des fins de prospections commerciales ou de publicité, par exemple, le second doit s'entendre comme étant la possibilité pour la personne concernée de demander que cesse le traitement de ses renseignements pour les fins mentionnées lors de la collecte. Ces deux approches illustrent les conceptions européenne et américaine du commerce électronique en ce qui concerne le traitement des renseignements personnels.

Ainsi, eu égard au principe et à la réponse donnée dans la FAQ 12, le régime général institué par les *Safe Harbor Principles* fait référence à l'*opt-out*. En effet, il est indiqué que,

> [d]'*une manière générale, le principe du choix a pour but d'assurer que les informations à caractère personnel sont utilisées et communiquées conformément aux attentes et aux choix de la personne concernée. Par conséquent, lorsque des informations à caractère personnel sont utilisées dans le cadre d'une action de* marketing *direct, toute personne concernée devrait pouvoir exercer son droit de refus (ou de choix) à tout moment, dans certaines limites définies par l'organisation (par exemple, délai pour permettre à l'organisation d'appliquer le refus).*[28]

Dès lors, pour exprimer leur droit d'opposition *a posteriori* « des mécanismes clairs et visibles, d'accès facile et d'un coût raisonnable » doivent être offerts aux personnes concernées.

---

[27] ARTICLE 29 GROUPE DE PROTECTION DES DONNÉES, *id*. En 1999, il était indiqué qu' « au stade actuel, la combinaison de la notification et du choix débouche sur la possibilité d'utiliser des données à des fins autres que celles notifiées et ce, sans obligation de laisser le choix (à moins que ces fins soient incompatibles ou que les données soient sensibles), ce qui est contraire aux lignes directrices de l'OCDE (principe de limitation de l'utilisation). Le groupe de travail soutient l'idée que le choix doit être offert lorsque les données sont utilisées à des fins compatibles, mais différentes. », p. 8.

[28] FAQ 12, Annexe 1 – Principes de la « sphère de sécurité » relatifs à la protection de la vie privée publiés par le ministère américain du commerce le 21 juillet 2000 de la Décision du 26 juillet 2000, *op. cit*. note 7.

Toutefois, on peut regretter que la FAQ 12 ne fasse mention que du *marketing* direct, certes il s'agit là d'un enjeu de taille si l'on considère l'affaire *DoubleClick*, mais ce n'est pas « un cas non unique »[29] comme le montre, par exemple, la problématique du pollupostage.

En plus de chercher à obtenir le consentement de la personne concernée, le responsable du traitement doit veiller, lors de transferts ultérieurs, à ce que le tiers destinataire des renseignements personnels respecte les principes de la « sphère de sécurité ».

Transfert ultérieur

Transfert ultérieur
Le responsable du traitement doit certifier auparavant que le tiers destinataire des données : • souscrit aux principes de la sphère de sécurité ou; • est soumis aux dispositions de la directive ou d'un autre mécanisme attestant le niveau adéquat de la protection ou, • a conclu un accord dans lequel il s'engage à assurer au moins le même niveau de protection. Le responsable ne pourra alors faire l'objet d'une plainte si le tiers ne respecte pas les principes, sauf s'il le savait ou aurait dû le savoir et qu'il n'a rien fait pour éviter un traitement contraire aux principes.
➥ responsabilité (*OCDE - Directive 95/46/CE*); qualité des données (*Convention 108*)

L'énonciation de ce principe vise à responsabiliser les entreprises et organisations qui entendent communiquer les renseignements personnels qu'ils détiennent sur un individu. Une telle communication ne pourra donc se faire que si le tiers destinataire s'est au préalable engagé à respecter les principes de la « sphère de sécurité ». On retrouve dans ce principe la *philosophie* de l'article 25 de la *Directive 95/46/CE*, à savoir que le transfert de renseignements personnels ne peut se faire que si le pays, l'entreprise ou organisation destinataire offre un niveau de protection adéquat. Il a souvent été rappelé lors des négociations que

> […] *ce principe est nécessaire pour assurer que les données ne sont pas transférées par une société américaine qui observe les principes de la « sphère de sécurité » à un responsable du traitement américain ou autre, ne garantissant pas un niveau de protection adéquat.* [30]

La responsabilisation des entreprises et organisations doit s'entendre non seulement lors du transfert, mais aussi à la suite de ce dernier. Ainsi, si le responsable du traitement savait ou aurait dû savoir que le tiers destinataire des données ne respecte pas les principes de la « sphère de sécurité » et qu'il n'a pas pris les mesures nécessaires pour mettre fin à une telle contravention, dans ce cas, sa responsabilité pourra être engagée. Cette mesure incite donc le responsable de traitement à mettre en place des mécanismes garantissant la confidentialité et la sécurité des renseignements personnels[31].

---

[29] Yves POULLET, « Les Safe Harbor Principles – Une protection adéquate? », *Droit et Nouvelles Technologies*, 10 juillet 2000, http://www.droit-technologie.org/2_1.asp?dossier_id=24, p. 11.

[30] ARTICLE 29 GROUPE DE PROTECTION DES DONNÉES, *Avis 2/99 concernant la pertinence des « principes internationaux de la sphère de sécurité » publiés par le ministre du commerce des Etats-Unis le 19 avril 1999*, WP 19, 3 mai 1999, http://www.europa.eu.int/comm/internal_market/privacy/docs/wpdocs/1999/wp19fr.pdf.

[31] Pour une illustration des interrogations soulevées par ce principe, voir notamment : ARTICLE 29 GROUPE DE PROTECTION DES DONNÉES, *Avis 7/99*, *op. cit.* note 26. Les auteurs de cet avis préconisaient « de reconsidérer l'impunité de l'auteur du transfert, de reconnaître la responsabilité de ce dernier en cas de négligence et

Sécurité

Sécurité
Le responsable du traitement doit prendre les mesures nécessaires pour éviter la perte, l'utilisation abusive, la consultation illicite, la divulgation, la modification et la destruction des données.
➥ garanties de sécurité (*OCDE*); sécurité des données (*Convention 108*); confidentialité et sécurité des traitements (*Directive 95/46/CE*)

Le traitement des renseignements personnels doit se faire dans un environnement sécuritaire. Le responsable du traitement doit donc mettre en œuvre des mesures matérielles, administratives et techniques pour assurer la sécurité des données[32]. Ces mesures auront pour effet d'éviter toute malversation lors du traitement de ces dernières.

L'adoption de telles mesures visera à protéger les renseignements personnels contre l'utilisation, la communication, l'accès non autorisé ainsi que contre la copie, l'altération, la perte, la destruction accidentelle ou illicite. Pour éviter de telles atteintes, il revient au responsable du traitement de veiller à ce que les mesures employées respectent les règles de l'art et offrent un niveau de sécurité approprié au traitement et à la nature des renseignements colligés.

Par ailleurs, une fois les renseignements personnels collectés, le responsable du traitement doit assurer la sécurité de ses bases de données. En effet, seules les personnes autorisées doivent avoir la possibilité de consulter et de modifier lesdits renseignements. Les accès aux bases de données doivent donc être restreints.

---

d'imprudence et de le contraindre à aider la personne concernée à trouver une solution », p. 8; *Avis 4/2000*, *op. cit.* note 24, p. 6.

[32] *Lignes directrices de l'OCDE*, précité note 5. Aux termes du § 56 de l'Exposé des motifs, « les notions de sécurité et de protection de la vie privée n'ont pas la même signification. Cependant, les limitations imposées à l'utilisation et à la divulgation des données devraient être renforcées par des garanties de sécurité. Ces garanties comprennent des mesures d'ordre matériel (verrouillage des portes et cartes d'identification, par exemple), des mesures structurelles (telles que les niveaux hiérarchiques en ce qui concerne l'accès aux données) et, en particulier avec les systèmes informatiques, des mesures informationnelles (telles que le chiffrement et la surveillance des activités inhabituelles susceptibles de présenter un danger et des mesures destinées à y faire face). I1 conviendrait de souligner que la catégorie des mesures structurelles comprend l'obligation faite au personnel chargé du traitement de l'information de maintenir le caractère confidentiel des données. » ; Vincent GAUTRAIS, « Les aspects relatifs à la sécurité », dans Daniel POULIN, Éric LABBÉ, François JACQUOT et Jean-François BOURQUE, *Guide juridique du commerçant électronique*, Montréal, Thémis, 2003. Avant d'examiner les différentes formes de sécurité, l'auteur précise que « malgré l'importance croissante que les acteurs lui accordent actuellement, la sécurité des réseaux informatiques demeure la moins organisée et la plus négligée des quatre principales dimensions du commerce électronique (juridique, commercial, technique et sécurité). Responsable d'une école en sécurité informatique, Nicolas SADIRAC prétend à ce titre que les entreprises se contentent de propagande et occultent l'ignorance de la population quant aux problèmes de sécurisation des transactions. Le succès de certains pirates informatiques à interrompre le fonctionnement de sites commerciaux réputés semblent lui donner raison. D'ailleurs, les spécialistes s'accordent sur le fait que la question n'est pas de savoir qui va être touché par des intérêts malveillants (hacking) ou négligents mais plutôt quand. », p. 75.

Accès

Accès
Les personnes concernées doivent avoir accès à leurs données, et doivent pouvoir les corriger, les modifier ou les supprimer lorsqu'elles sont inexactes, sauf si demande disproportionnée par rapport aux risques pesant sur la vie privée de la personne concernée ou susceptible d'entraîner une violation des droits d'autres personnes.
➥ participation individuelle (*OCDE*); garanties complémentaires pour la personne concernée (*Convention 108*); droit d'accès (*Directive 95/46/CE*)

Le principe de l'accès doit s'entendre comme étant le droit pour les personnes concernées de consulter leur dossier et d'en obtenir une copie compte tenu du fait que

> […] *l'accès constitue un principe fondamental de tout régime de protection des données sérieux car c'est ce qui déclenche le recours à tous les droits de la personne concernée*.[33]

Par conséquent, toute personne physique doit avoir la possibilité de connaître quelles sont les renseignements la concernant qu'une entreprise ou une organisation détient sur elle. L'exercice de ce droit doit s'effectuer selon les modalités expliquées dans la FAQ 8 en ce qui concerne, entre autres :

- le caractère absolu ou non du droit d'accès;
- les informations commerciales confidentielles;
- les exceptions au droit d'accès. Concernant ce point, il avait été noté lors des discussions que « la règle générale consiste à octroyer un accès sous réserve de certaines exceptions. Ces exceptions devraient être énoncées précisément dans le texte [du principe, ou encore dans les FAQ] »[34];
- le coût de l'exercice du droit d'accès;
- l'accès aux informations publiques, et
- le délai de réponse.

L'exercice du droit d'accès permet donc à la personne concernée d'obtenir communication des renseignements la concernant détenus par une entreprise ou une organisation. À partir de là, elle peut vouloir faire rectifier certaines informations contenues dans son dossier afin d'assurer l'exactitude et l'intégrité des données qui serviront à prendre une décision à son encontre.

[33] ARTICLE 29 GROUPE DE PROTECTION DES DONNÉES, *Avis 7/99*, *op. cit.* note 26, p. 9.
[34] ARTICLE 29 GROUPE DE PROTECTION DES DONNÉES, *Avis 2/99*, *op. cit.* note 30, p. 6.

Intégrité des données

Intégrité des données
Les données collectées doivent être pertinentes pour les utilisations auxquelles elles sont destinées et elles ne doivent pas être utilisées d'une manière incompatible avec les objectifs initiaux ou ceux approuvés ultérieurement par la personne concernée. Le responsable du traitement doit assurer la fiabilité des données par rapport à l'utilisation prévue ainsi que leur exactitude, leur exhaustivité et leur actualité.
➥ qualité des données (*OCDE – Convention 108 – Directive 95/46/CE*)

Le principe de l'intégrité des données signifie que seuls les renseignements pertinents, nécessaires et non excessifs par rapport à l'objet du traitement doivent être collectés par le responsable du traitement. Cette idée de nécessité correspond au principe de qualité des données sous entendant qu'il est important que les renseignements personnels collectés soient en accord avec les finalités poursuivies par le responsable du traitement.

Mise en œuvre

Mise en œuvre
Nécessité de mettre au point des mécanismes permettant d'assurer le respect des principes, de ménager un droit de recours aux personnes concernées par le non-respect des principes et de sanctionner les responsables du traitement qui n'ont pas appliqué les principes alors qu'ils s'y sont engagés.
➥ mise en œuvre des principes à l'échelon national (*OCDE*); sanctions et recours (*Convention 108*); recours juridictionnels, responsabilité et sanctions (*Directive 95/46/CE*)

L'adhésion aux principes de la « sphère de sécurité » est volontaire et se fait sur la base d'une déclaration rendue publique, sur le site du ministère du commerce américain, dans laquelle le responsable du traitement s'engage à respecter les principes énoncés ci-dessus, sous peine de voir ses pratiques sanctionnées par la *Federal Trade Commission* (ci-après « FTC »), par exemple.

Cette situation – adhésion volontaire et contrôle par la *FTC* – qui est présentée comme étant un « « *effective mix* », c'est-à-dire un système alliant les vertus de l'autoréglementation et l'autorité de la puissance publique »[35], a été au centre des discussions entre l'Union européenne et les États-Unis.

Concernant l'adhésion aux principes de la « sphère de sécurité », les critiques ont souvent porté sur le caractère volontaire des engagements, l'absence de contrôle des intentions du responsable du traitement par une autorité, l'absence de recours et de sanctions pour garantir l'efficacité d'un tel mécanisme. Ces critiques ont conduit à la rédaction du principe de la mise en œuvre et aux précisions contenues dans la FAQ 6, à savoir que l'engagement du responsable du traitement doit contenir

[35] POULLET Y., *loc. cit.*, note 29 (les italiques de l'auteur).

[…] *au moins les informations suivantes :*

1) le nom de l'organisation, son adresse postale, son adresse électronique, ses numéros de téléphone et de télécopieur;

2) *une description des activités de l'organisation relativement aux informations à caractère personnel en provenance de l'Union européenne;*

3) *une description des dispositions de protection de la vie privée appliquées par l'organisation auxdites informations, précisant : a) le lieu où le texte de ces dispositions peut être consulté par le public; b) la date de mise en œuvre de ces dispositions; c) le service à contacter en cas de plainte, pour des demandes d'accès et pour toute autre question relevant de la « sphère de sécurité »; d) le nom de l'instance réglementaire spécifique qui est chargée de statuer sur les plaintes déposées, le cas échéant, contre l'organisation pour pratiques déloyales ou frauduleuses et pour infraction aux lois ou aux réglementations régissant la protection de la vie privée (…); e) l'intitulé de tout programme relatif à la protection de la vie privée auquel participe l'organisation; f) la méthode de vérification (par exemple, en interne ou par des tiers) et g) l'instance de recours indépendante qui pourra instruire les plaintes non résolues.*[36]

Par cet engagement, renouvelé chaque année et rendu public sur le site du ministère américain du commerce[37], on retrouve l'esprit des politiques de confidentialité et de la certification, ces deux instruments volontaires matérialisant les intentions des responsables du traitement des renseignements personnels. Dans le premier cas, on parle de labellisation interne, dans le second de labellisation externe faisant intervenir une tierce personne.

En recourant à la labellisation externe, le responsable du traitement s'engage à respecter les règles mises en place par une autorité de certification, de type TRUSTe[38] ou BBBOnLine[39]. Par exemple, à côté du *Privacy Seal Program*[40], TRUSTe a mis en place l'*EU Safe Harbor Program*[41] proposant deux services : un conduisant à la labellisation de l'entreprise ou de l'organisme, un autre offrant un mécanisme alternatif de résolution – hors et en ligne – des conflits relatifs au traitement de renseignements personnels.

Un tel mécanisme de résolution des conflits n'est pas exclusif[42]. Ainsi, si une entreprise ou une organisation ne se conforme pas à la décision prise par une autorité de certification, cette dernière peut soumettre l'affaire à la *FTC* qui

[…] *s'est engagée à examiner en priorité les cas soumis par les organisations d'autoréglementation, telles que BBBOnline et TRUSTe, ainsi que par les États membres*

---

[36] FAQ 6, Annexe 1 – Principes de la « sphère de sécurité » relatifs à la protection de la vie privée publiés par le ministère américain du commerce le 21 juillet 2000 de la Décision du 26 juillet 2000, *op. cit.* note 7. Ce principe doit se lire parallèlement aux FAQ 7 (Vérification) et 11 (Résolution des conflits et application des décisions).

[37] 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.

[38] http://www.truste.net.

[39] http://www.bbbonline.org.

[40] http://www.truste.net/programs/pub_how.html.

[41] http://www.truste.net/programs/pub_harbor.html.

[42] À ce sujet, il convient de préciser que les entreprises et organisations américaines peuvent souhaiter coopérer avec les autorités de l'Union européenne chargées de la protection des données quant à l'application des principes de la « sphère de sécurité » comme mentionné dans la FAQ 5, Annexe 1 – Principes de la « sphère de sécurité » relatifs à la protection de la vie privée publiés par le ministère américain du commerce le 21 juillet 2000 de la Décision du 26 juillet 2000, *op. cit.* note 7.

de l'Union européenne en ce qui concerne le non-respect des principes de la « sphère de sécurité », afin de déterminer s'il y a eu une violation de la section 5 du Federal Trade Commission Act, qui interdit les actions ou pratiques déloyales ou frauduleuses dans le commerce. [43]

Conformément aux recommandations formulées en mai 2000 par l'Article 29 Groupe de protection des données[44], le lien entre ces deux niveaux a fait l'objet de précisions, notamment quant aux pouvoirs de la *FTC* en matière de protection de la vie privée[45] compte tenu du fait que

[d]*ans l'exercice de ses pouvoirs au titre de la section 5, la FTC considère que toute fausse déclaration sur les motifs de la collecte d'information auprès des consommateurs et sur la façon dont ces informations seront utilisées constitue une pratique frauduleuse.*[46]

Dès lors, si la *FTC* constate de une telle pratique, elle peut émettre « une ordonnance de cessation » en vue de mette fin au comportement infractionnel (15 USC, § 45 a) 2), édicter des prescriptions administratives en cas de non-respect persistant (15 USC, § 57 a)) ou faire prononcer des astreintes (15 USC, § 45 1 et § 45m).

En plus des prescriptions administratives pouvant être prise en cas de non-respect persistant des engagements par une entreprise ou une organisation, la *FTC* devra informer le ministère du commerce de cette situation qui

[…] *introduira dans la liste publique, tenue par lui, des organisations déclarant leur adhésion aux principes de la « sphère de sécurité » toute notification de non-respect persistant, (…) mais seulement après avoir accordé à l'organisation concernée un préavis de trente (30) jours et la possibilité de répondre. La liste publique tenue par le ministère du commerce précisera donc quelles organisations bénéficient des avantages de la « sphère de sécurité » et quelles organisations n'en bénéficient plus.*[47]

Suite à l'analyse des *Safe Harbor Principles*, il convient d'envisager la portée de ces derniers, étant entendu, d'une part, conformément à la décision rendue le 26 juillet 2000 par la Commission européenne, qu'une adaptation peut intervenir à tout moment et, d'autre part, qu'une évaluation doit avoir lieu trois ans après leur entrée en vigueur[48].

II. Portée des *Safe Harbor Principles*

Victoire pour les uns, échec pour les autres, un compromis fait rarement l'unanimité. Les principes de la « sphère de sécurité » n'échappent pas à cette situation comme l'illustrent les nombreuses analyses faites au lendemain de leur adoption. Cependant, plus de trois ans après leur entrée en vigueur, et en attendant le rapport d'évaluation de la Commission européenne, il est possible de noter que même si leur application reste limité, les principes de la « sphère de

[43] FAQ 11 (Action de la FTC), Annexe 1 – Principes de la « sphère de sécurité » relatifs à la protection de la vie privée publiés par le ministère américain du commerce le 21 juillet 2000 de la Décision du 26 juillet 2000, *id*.

[44] ARTICLE 29 GROUPE DE PROTECTION DES DONNÉES, *Avis 4/2000*, *op. cit*. note 24, p. 7

[45] Annexe III – Étude relative à la mise en œuvre des principes de la « sphère de sécurité », *op. cit*. note 7.

[46] Annexe III – Étude relative à la mise en œuvre des principes de la « sphère de sécurité », *id*.

[47] FAQ 11 (Non-respect persistant), Annexe 1 – Principes de la « sphère de sécurité » relatifs à la protection de la vie privée publiés par le ministère américain du commerce le 21 juillet 2000 de la Décision du 26 juillet 2000, *id*.

[48] *Décision du 26 juillet 2000*, article 4 (1), *id*.

sécurité » constituent un pas en avant pour la protection des renseignements personnels dans les environnements en réseaux.

Une application limitée …

Un peu plus de 100 organisations à la fin 2001 et un peu moins de 500 en avril 2004, tel est le nombre d'organisations ayant publiquement adhérés aux principes de la « sphère de sécurité ». Cette relative progression n'est pas sans rappeler celle des politiques de confidentialité aux débuts des années 2000. Alors qu'en 1998, 14% des 1400 sites examinés par la *FTC* disposaient d'une politique envers le traitement des renseignements personnels[49], les enquêtes menées par la suite ont démontré que ce nombre allait croissant, notamment sous la menace d'intervention du Congrès américain au lendemain du rapport de 2000 de la *FTC* qui tout en reconnaissant le rôle de l'autoréglementation dénonçait la faible sensibilisation des entreprises en ligne à ce mode d'action[50].

Cette relative progression quant aux politiques de confidentialité ou à l'adhésion aux principes de la « sphère de sécurité » peut s'expliquer, d'une part, par l'attitude attentiste des entreprises et organisations américaines vis-à-vis de la protection et du transfert des renseignements personnels. Attentisme afin de savoir si les grandes entreprises vont s'engager dans un ce chemin. En l'espèce, le nombre d'adhésion a augmenté lorsque *Microsoft* et *TRUSTe* ont annoncé leur intention à s'engager dans la « sphère de sécurité », soit à la mi-2001. Attentisme face à la volonté des gouvernements et des autorités de contrôle, comme la *FTC* ou la Commission européenne, quant à l'application des principes.

D'autre part, cette relative progression s'explique au regard des activités entrant dans le champ d'action de la « sphère de sécurité » comme le souligne Joël R. Reidenberg dans les termes suivants :

> [n]*otwithstanding its validity in either legal system, the scope of Safe Harbor provision is very narrow. First, Safe Harbor by its terms can only apply to activities and U.S. organizations that fall within the regulatory jurisdiction of the FTC and the U.S. Department of Transportation. As a result, many companies and sectors will be ineligible for Safe Harbor, including particularly the banking, telecommunications, and employment sectors that are expressly excluded from the FTC's jurisdiction. Second, Safe Harbor will not apply to most organizations collecting data directly in Europe. Article 4 of the European Directive provides that, if a data controller is located outside of the European Union but uses equipment within the European Union, the law of the place where the equipment is located will be applicable.*[51]

Dès lors, on peut se demander si cette situation n'est pas de nature à créer une disparité entre les entreprises et organisations américaines susceptibles d'adhérer aux principes de la « sphère de

---

[49] FEDERAL TRADE COMMISSION, *Privacy Online : A Report to Congress*, juin 1998, http://www.ftc.gov/reports/privacy3/toc.htm.

[50] FEDERAL TRADE COMMISSION, *Privacy Online : Fair Information Practices in the Electronic Marketplace. A Report to Congress*, mai 2000, http://www.ftc.gov/reports/privacy2000/privacy2000.pdf.

[51] Joël R. REIDENBERG, « E-commerce and Trans-Atlantic Privacy », (2001) 38 *Houston Law Review*, 717-749, 743.

sécurité » et les autres qui ne relèvent pas de la *FTC* et du ministère des transports. Ainsi, l'adoption des *Safe Harbor Principles*, visant à réduire l'absence d'homogénéité entre l'Union européenne et les États-Unis par la reconnaissance de principes minimaux quant à la protection des renseignements personnels, ne serait-elle pas source d'hétérogénéité au sein même des États-Unis? Toutefois, la logique sectorielle d'encadrement du traitement des renseignements personnels aux États-Unis n'est-elle pas déjà source d'hétérogénéité et rien n'empêche les entreprises et organisations ne relevant pas de la *FTC* ou du ministère des transports de reprendre les principes énoncés dans les politiques de confidentialité ou de choisir la voie contractuelle lors du transfert de renseignements personnels avec l'Union européenne.

Enfin, cette solution peut également expliquer la relative progression des adhésions. En effet, l'article 26 de la *Directive 95/46/CE* reconnaît un certain nombre de dérogations permettant aux entreprises et organisations américaines de se conformer aux exigences de la « sphère de sécurité ». Ainsi, il est possible de transférer des renseignements personnels vers un pays tiers n'assurant pas un niveau de protection adéquat, si, par exemple, la personne concernée y a indubitablement consenti[52] ou que celui-ci soit nécessaire à la sauvegarde soit d'un intérêt public important[53], soit de l'intérêt vital de la personne concernée[54]. Un tel transfert est également possible

> […] *lorsque le responsable du traitement offre des garanties suffisantes au regard de la protection de la vie privée et des libertés et droits fondamentaux des personnes, ainsi qu'à l'égard de l'exercice des droits correspondants; ces garanties peuvent notamment résulter de clauses contractuelles appropriées*.[55]

Pour être approuvé[56], il est important que les trois principes suivants soient compris dans le contrat pour assurer un niveau minimum de protection : 1) seuls les renseignements nécessaires à la réalisation de l'objet doivent être collectés, 2) les utilisations et/ou les transferts ultérieurs doivent être circonscrits aux finalités initiales et, 3) les personnes concernées doivent pouvoir exercer leurs droits d'accès et de rectification tant à l'égard de l'expéditeur que du destinataire des données[57]. De plus, le contrat doit contenir des dispositions relatives aux voies de recours offertes à la personne concernée en cas de lésion.

Tenant compte des travaux l'Article 29 Groupe de protection des données, la Commission européenne a adopté, en juin 2001, la *Décision relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des pays tiers en vertu de la Directive*

---

52 *Directive 95/46/CE*, article 26 alinéa 1 (a).

53 *Directive 95/46/CE*, article 26 alinéa 1 (d).

54 *Directive 95/46/CE*, article 26 alinéa 1 (e).

55 *Directive 95/46/CE*, article 26 alinéa 2.

56 Dans ses prises de décisions, la Commission est assistée par le Comité institué par l'article 31 de la *Directive 95/46/CE* et composé des représentants des États membres. Ce comité émet des avis sur les projets de la Commission. La Commission peut ne pas suivre les avis rendus par le comité. Dans ce cas, elle doit immédiatement communiquer au Conseil la mesure litigieuse et en suspendre l'application jusqu'à la décision du Conseil.

57 ARTICLE 29 GROUPE DE PROTECTION DES DONNÉES, *Avis 1/2001 sur le projet de décision de la Commission sur les clauses contractuelles types concernant le transfert de données à caractère personnel vers des pays tiers en vertu de l'article 26, paragraphe 4, de la directive 95/46*, WP 38 finale, 26 janvier 2001, http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2001/wp38fr.pdf.

95/46/CE[58]. Cette décision, dans l'attente de l'examen des législations relatives à la protection des renseignements personnels dans les pays tiers, permettra la continuité des relations commerciales entre les pays Membres de l'Union européenne et les pays tiers, étant entendu aux termes de l'article 1er de cette décision que

> […] *les clauses contractuelles types contenues dans l'annexe sont considérées comme offrant des garanties suffisantes en matière de protection de la vie privée et des droits fondamentaux et des libertés des individus et en ce qui concerne l'exercice des droits correspondants comme l'exige l'article 26, paragraphe 2, de la directive 95/46/CE.*

Par conséquent, si l'exportateur et l'importateur de données ne veulent pas voir leurs flux transfrontières être interdits ou suspendus, il leur est fortement recommandé d'insérer les clauses types dans leurs contrats. Le recours aux clauses contractuelles est, en effet, considéré comme étant l'un des moyens d'offrir un niveau de protection adéquat aux données transférées vers des pays tiers, comme cela a également été admis par l'adoption par le Conseil de l'Europe d'un *contrat-type visant à assurer une protection équivalente des données dans le cadre des flux transfrontières de données*[59]. Ce dernier a pour but d'encadrer les échanges intervenant entre parties soumises à des protections juridiques différentes, étant entendu selon l'article 24 que

> *[…] les clauses du contrat-type ont été conçues pour permettre le transfert de données à caractère personnel entre des entités économiques indépendantes. Le soin est laissé aux parties de décider d'avoir ou non recours aux clauses; celles-ci sont facultatives. Les parties doivent les adapter à des conditions spécifiques. Les clauses peuvent servir de fondement à l'instauration et au développement de règles appropriées, par exemple pour des transferts au sein du même groupe d'entreprises ou entre le maître d'un fichier et un service de traitement.*

Toutes ces explications permettent de relativiser l'application limitée des principes de la « sphère de sécurité ». En effet, s'il est possible de croire que les entreprises et les organisations sont peu sensibilisées au regard du nombre d'adhésions, il ne faut pas pour autant nier que la reconnaissance du niveau de protection adéquat offert par ces principes constitue un pas en avant et est source d'influence en la matière.

---

[58] COMMISSION EUROPÉENNE, *Décision C(2001) 1539 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*, J. O. des Communautés européennes n° L181 du 4 juin 2001, pp. 19-31, http://europa.eu.int/comm/internal_market/privacy/modelcontracts_fr.htm. Notons que ces clauses, aux termes de l'article 2 pargraphe 2 de la présente décision « ne s'applique pas au transfert de données à caractère personnel par des responsables du traitement établis dans la Communauté à des tiers établis en dehors de la communauté qui agissent seulement comme sous-traitants ». Relativement à ce type de relation, il est possible de se référer à : COMMISSION EUROPÉENNE, *Décision 2002/16/CE 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 95/46/CE*, J. O. des Communautés européennes n° L6 du 10 janvier 2002, pp. 52-66, http://europa.eu.int/comm/internal_market/privacy/modelcontracts_fr.htm.

[59] CONSEIL DE L'EUROPE, *Contrat-type visant à assurer une protection équivalente des données dans le cadre des flux transfrontières de données*, 1992, http://www.coe.int/T/F/Affaires_juridiques/Coop%E9ration_juridique/Protection_des_donn%E9es/Documents/Publications/1ContratType.asp#TopOfPage. Voir, aussi : Jérôme HUET, « Les contrats encadrant les transferts de données personnelles », *Communication. Commerce électronique*, mai 2001, n° 5, 8-14.

… ayant néanmoins une certaine influence

Nonobstant les zones d'incertitude ou les questions soulevées par l'entrée en vigueur des principes de la « sphère de sécurité », ces derniers visent à sensibiliser les entreprises et organisations américaines à la problématique de la protection des renseignements personnels. Cette sensibilisation est nécessaire à l'établissement d'un climat de confiance non seulement auprès des personnes concernées par le traitement de leurs renseignements personnels, mais aussi des autorités – publiques et privées – chargées de veiller à l'application desdits principes. Un tel sentiment, pour être entier, doit s'envisager aussi bien individuellement que collectivement. C'est pourquoi, il est important que les entreprises et organisations américaines reconnaissent la valeur de ces principes qui, avant d'être « ceux » de la *Directive 95/46/CE*, reprennent, dans une certaine mesure, les dispositions contenues dans les *Lignes directrices de l'OCDE* reconnues par les États-Unis et confirmées à la conférence ministérielle sur le commerce électronique qui s'est tenue à Ottawa en octobre 1998[60].

Pour sensibiliser les entreprises et organisations, il est important que les associations professionnelles diffusent de l'information relative aux principes de la « sphère de sécurité » afin de promouvoir ces derniers. À cet effet, il est possible de se référer à l'action de la *Direct Marketing Association* (ci-après « DMA »)[61] proposant à ses membres un *DMA Safe Harbor Program*[62]. Il est indiqué, à l'intention des entreprises de *marketing* direct que :

> *The DMA has developed a program to assist those companies that wish to comply with the safe harbor requirements, and thus be able to certify to the Department of Commerce that it has fulfilled the requirements of the safe harbor principles. The DMA will:*
>
> ***Serve as your third-party dispute and enforcement mechanism**. European consumers, companies and governments can be assured that your company will adhere to the third-party dispute and enforcement requirements of the safe harbor framework. This will solidify Europeans' trust and confidence in your organization. (For a complete description regarding the DMA's process for handling complaints and serving as your independent enforcement mechanism, please refer to The DMA Safe Harbor Program Complaint Procedure fact sheet on our web site at: www.the-dma.org/safeharbor.)*
>
> ** **Provide members with assistance in developing a privacy policy that is based on the safe harbor privacy principles**. By adhering to those core principles of: notice, choice, onward transfer, access, security, data integrity and enforcement, your company is indicating that you place great value on data privacy protection and will make every effort to respect Europeans' requests regarding use of their personal information.*
>
> ** **Provide technical assistance and educational materials to assist you throughout the process for meeting the safe harbor requirements**. The DMA stands ready to assist your company in:*
>
> *(1) meeting the Department of Commerce's registration requirements for safe harbor,*
> *(2) setting up an in-house dispute resolution system to handle potential customer complaints,*
> *(3) serving as your independent third-party dispute resolution mechanism, and*

60 http://www.ottawaoecdconference.org.
61 http://www.the-dma.org.
62 http://www.the-dma.org/safeharbor/index.html.

(4) addressing any other questions or concerns your company has regarding the safe harbor process.

* ***Provide a DMA Safe Harbor Program mark****. This mark will provide consumers with an easily recognizable symbol that signifies and distinguishes your organization as being in compliance with the safe harbor enforcement principle.*[63]

Cette initiative de la *DMA* s'inscrit dans la lignée des codes de conduite mise en place par cette association à l'attention de ses membres, action encouragée par la *Directive 95/46/CE*[64]. Par ailleurs, en plus de cette sensibilisation permettant l'établissement d'un climat de confiance, nécessaire au commerce électronique, les principes de la « sphère de sécurité » influencent certaines initiatives à l'image du *EU Safe Harbor Program* de *TRUSTe*.

Ainsi, la *FTC* a approuvé la validité de trois programmes visant à garantir la protection des renseignements personnels des enfants de moins de 13 ans, comme ceux proposés par le *Children's Advertising Review Unit of the Council of Better Business Bureau* (CARU)[65], l'*Entertainment Software Rating Board*[66] ou *TRUSTe*[67]. Elle examine actuellement la demande[68] de la société Privo[69] considérant que

Privo, Inc. has created a proprietary technology platform that enables participating companies to initiate and manage responsible relationships with their online consumers through an identity and permission management platform. The platform, the PrivoLock™ System, allows consumers, or registrants, to maintain control of their personally identifiable information, edit its content, and extend this privacy protection to their children while providing companies with a legally compliant "opt-in" marketing database for communicating with their customers.

Privo extends to multiple industries that market family-oriented products and services and to general audience websites that attract kids. It is a costly challenge for individual companies to responsibly and legally initiate and sustain online interactive communication with kids. Privo enables these companies to create lifetime customer relationships through branded permission-management systems consistent with the Children's Online Privacy Protection Act (COPPA).[70]

---

63 http://www.the-dma.org/safeharbor/businesses.shtml.

64 *Directive 95/46/CE*, article 27.

65 FEDERAL TRADE COMMISSION, « Re : Application of Children's Advertising Review Unit Children's Online Privacy Protection Rule Safe Harbor Program », 26 janvier 2001, http://www.ftc.gov/os/2001/02/caruletter.pdf; « CARU Safe Harbor Program Requirements and Compliance Checklist », http://www.ftc.gov/privacy/safeharbor/carureqs.pdf.

66 FEDERAL TRADE COMMISSION, « Re : Application of ESRB, Children's Online Privacy Protection rule Safe Harbor Program », 18 avril 2001, http://www.ftc.gov/privacy/safeharbor/esrbapprovalltr.htm.

67 FEDERAL TRADE COMMISSION, « Re : Application of TRUSTe, Children's Online Privacy Protection Rule Safe Harbor Program », 21 mai 2001, http://www.ftc.gov/privacy/safeharbor/trusteapprovalltr.htm.

68 FEDERAL TRADE COMMISSION, « FTC Seeks Public Comment on Privo, Inc.'s Application For Approval as a « Safe Harbor » Program under the Children's Online Privacy Protection Rule », 2 avril 2004, http://www.ftc.gov/opa/2004/04/privo.htm.

69 http://www.privo.com.

70 http://www.privo.com/about.htm.

À l'image de ces initiatives, il est possible de considérer que même si l'application des *Safe Harbor Principles* ne rencontre pas toutes les exigences, ceux-ci constituent néanmoins un pas en avant pour la protection des renseignements personnels entre l'Union européenne et les États-Unis.

Conclusion

Par cette analyse des *Safe Harbor Principles*, nous avons voulu montrer que la protection des renseignements personnels dans les environnements en réseaux doit s'envisager de plusieurs manières – lois, politiques de confidentialité, labels, codes de conduite, contrats … pourvu que celles-ci prennent en considération un certain nombre de principes reconnus comme offrant un niveau de protection jugé équivalent, adéquat, ou encore similaire. Le contenu de la protection ne doit-il pas primer sur son contenant?

En partant de cette idée, il est possible de conclure en disant qu'au regard des différences entre l'Union européenne et les États-Unis, la reconnaissance de ces principes a pour objet, d'une part, d'aplanir non seulement l'hétérogénéité des législations protectrices mais aussi les logiques territoriales car ceux-ci s'inscrivent dans un ensemble, celui de la « sphère de sécurité » et, d'autre part, de réduire l'aterritorialité des atteintes par la mise en place de mécanismes appropriés.

Bibliographie

Chapitres de livres

GAUTRAIS V., « Les aspects relatifs à la sécurité », dans Daniel POULIN, Éric LABBÉ, François JACQUOT et Jean-François BOURQUE, *Guide juridique du commerçant électronique*, Montréal, Thémis, 2003, p. 129 et suiv.

Articles de revues

CADOUX L., « La protection des données personnelles en dehors de l'Europe communautaire », dans *Revue française d'administration publique*, n° 89, janvier-mars 1999, 83-94.

HUET J., « Les contrats encadrant les transferts de données personnelles », *Communication. Commerce électronique*, mai 2001, n° 5, 8-14.

POULLET Y., « Les Safe Harbor Principles – Une protection adéquate? », *Droit et Nouvelles Technologies*, 10 juillet 2000, <http://www.droit-technologie.org/2_1.asp?dossier_id=24>

REIDENBERG J. R., « E-commerce and Trans-Atlantic Privacy », (2001) 38 *Houston Law Review*, 717-749, 743.

Documents publics

ARTICLE 29 GROUPE DE PROTECTION DES DONNÉES,

Document de travail : Évaluation des codes d'autoréglementation sectoriels : quand peut-on dire qu'ils contribuent utilement à la protection des données dans un pays tiers?, WP 7, 14 janvier 1998
<http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/1998/wp7_fr.pdf>

Document de travail : Vues préliminaires sur le recours à des dispositions contractuelles dans le cadre de transferts de données à caractère personnel vers des pays tiers, WP 9, 22 avril 1998
<http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/1998/wp9_fr.pdf>

Document de travail : Transfert des données personnelles vers des pays tiers : application des articles 25 et 26 de la directive relative à la protection des données, WP 12, 24 juillet 1998
<http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/1998/wp12_fr.pdf>

Avis 1/99 concernant le niveau de protection des données à caractère personnel aux Etats-Unis et les discussions en cours entre la Commission européenne et le gouvernement américain, WP 15, 26 janvier 1999
<http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/1999/wp15fr.pdf>

Avis 2/99 concernant la pertinence des « principes internationaux de la sphère de sécurité » publiés par le ministre du commerce des Etats-Unis le 19 avril 1999, WP 19, 3 mai 1999
<http://www.europa.eu.int/comm/internal_market/privacy/docs/wpdocs/1999/wp19fr.pdf>

Avis 7/99 sur le niveau de protection des données garanti par les principes de la « sphère de sécurité » publiés avec les questions fréquemment posées (FAQ) et d'autres documents connexes les 15 et 16 novembre 1999 par le ministère du commerce américain, WP 27, 3 décembre 1999
<http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/1999/wp27fr.pdf>

Avis 4/2000 sur le niveau de protection assuré par les « principes de la sphère de sécurité », WP 32, 16 mai 2000
<http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2000/wp32fr.pdf>

Avis 1/2001 sur le projet de décision de la Commission sur les clauses contractuelles types concernant le transfert de données à caractère personnel vers des pays tiers en vertu de l'article 26, paragraphe 4, de la directive 95/46, WP 38 finale, 26 janvier 2001
http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2001/wp38fr.pdf

Avis 6/2003 relatif au niveau de protection des données à caractère personnel dans l'Île de Man, WP 82, 21 novembre 2003
<http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2003/wp82_fr.pdf>

Avis 1/2004 sur le niveau de protection assuré en Australie à la transmission de données des dossiers passagers par les compagnies aériennes, WP 85, 16 janvier 2004
<http://europe.eu.int/comm/internal_market/privacy/docs/wpdocs/2004/wp85_fr.pdf>

Avis 2/2004 sur le niveau de protection adéquat des données à caractère personnel contenues dans les dossiers des passagers aériens (PNR) transférés au Bureau des douanes et de la protection des frontières des Etats-Unis (US CBP), WP 87, 29 janvier 2004
<http://europe.eu.int/comm/internal_market/privacy/docs/wpdocs/2004/wp87_fr.pdf>

Avis 3/2004 sur le niveau de protection assuré au Canada à la transmission, par les compagnies aériennes, des dossiers passagers et d'informations anticipés sur les voyageurs, WP 88, 22 février 2004
<http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2004/wp88_fr.pdf>

CONSEIL DE L'EUROPE, *Contrat-type visant à assurer une protection équivalente des données dans le cadre des flux transfrontières de données*, 1992,
<http://www.coe.int/T/F/Affaires_juridiques/Coop%E9ration_juridique/Protection_des_donn%E9es/Documents/Publications/1ContratType.asp#TopOfPage>

COMMISSION EUROPÉENNE,

Décision de la Commission du 26 juillet 2000 conformément à la directive 95/45/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, J.O. des Communautés européennes n° L 215 du 25 août 2000 p. 0007-0047.

Décision de la Commission du 26 juillet 2000 relative à la constatation, conformément à la directive 95/46/CE du Parlement européen et du Conseil, du caractère adéquat de la protection des données à caractère personnel en Suisse, J.O. des Communautés européennes n° L 215 du 25 août 2000 p. 0001-0003.

Décision de la Commission du 26 juillet 2000 relative à la constatation, conformément à la directive 95/46/CE du Parlement européen et du Conseil, du caractère adéquat de la

protection des données à caractère personnel en Hongrie, J.O. des Communautés européennes n° L 215 du 25 août 2000 p. 0004-0006.

Décision C(2001) 1539 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, J. O. des Communautés européennes n° L181 du 4 juin 2001, pp. 19-31
<http://europa.eu.int/comm/internal_market/privacy/modelcontracts_fr.htm>

Décision de la Commission du 20 décembre 2001 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 la loi canadienne sur la protection des renseignements personnels et les documents électroniques, J.O. des Communautés européennes n° L 2 du 4 janvier 2002 p. 0013-0016.

Décision 2002/16/CE 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 95/46/CE, J. O. des Communautés européennes n° L6 du 10 janvier 2002, pp. 52-66
<http://europa.eu.int/comm/internal_market/privacy/modelcontracts_fr.htm>

Décision de la Commission du 30 juin 2003 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'Argentine, J.O. des Communautés européennes n° L 168 du 5 juillet 2003.

Décision de la Commission du 21 novembre 2003 constatant le niveau de protection adéquat des données à caractère personnel à Guernesey, J.O. des Communautés européenne n° L 308 du 25 novembre 2003 p. 0027-0028.

ELECTRONIC PRIVACY INFORMATION CENTER, « EPIC Files FTC Complaint Against DoubleClick, Alleges « Deceptive and Unfair Trade Practice » in Online Data Collection », 10 février 2000
<http://www.epic.org/privacy/internet/ftc/DCLK_comp_pr.html>

FEDERAL TRADE COMMISSION,

Privacy Online : A Report to Congress, juin 1998
<http://www.ftc.gov/reports/privacy3/toc.htm>

Privacy Online : Fair Information Practices in the Electronic Marketplace. A Report to Congress, mai 2000
<http://www.ftc.gov/reports/privacy2000/privacy2000.pdf>

« Letter », 22 janvier 2001
<http://www.ftc.gov/os/closings/staff/doubleclick.pdf>

« Re : Application of Children's Advertising Review Unit Children's Online Privacy Protection Rule Safe Harbor Program », 26 janvier 2001
<http://www.ftc.gov/os/2001/02/caruletter.pdf>

« Re : Application of ESRB, Children's Online Privacy Protection Rule Safe Harbor Program », 18 avril 2001
<http://www.ftc.gov/privacy/safeharbor/esrbapprovalltr.htm >

« Re : Application of TRUSTe, Children's Online Privacy Protection Rule Safe Harbor Program », 21 mai 2001
<http://www.ftc.gov/privacy/safeharbor/trusteapprovalltr.htm>

In re DoubleClick Inc. Privacy Litigation (Objection by Settlement Class Members), 00-CIV-0641 (NRB) (U.S. District Court for the Southern District of New York)
<http://www.epic.org/privacy/cookies/doubleclickobjection.pdf>

In re DoubleClick Inc. Privacy Litigation, 00-CIV-0641 (NRB) (U.S. District Court for the Southern District of New York)
<http://www.nysd.uscourts.gov/courtweb/pdf/D02NYSC/01-03797.pdf>

« CARU Safe Harbor Program Requirements and Compliance Checklist »
<http://www.ftc.gov/privacy/safeharbor/carureqs.pdf>

« FTC Seeks Public Comment on Privo, Inc.'s Application For Approval as a « Safe Harbor » Program under the Children's Online Privacy Protection Rule », 2 avril 2004
<http://www.ftc.gov/opa/2004/04/privo.htm>

JUNKBUSTER, « DoubleClick, Abacus Direct and Privacy »,
<http://www.junkbusters.com/doubleclick.html>

THE SUPERIOR COURT OF THE STATE OF CALIFORNIA, Harriett Judnick v. DoubleClick Inc., Case No 000421
<http://www.arentfox.com/additionalsites/e-privacy/e-privacynews/privacy2000/Judnick.pdf>

Table des instruments légaux

PARLEMENT EUROPÉEN ET CONSEIL, *Directive 95/46/CE du Parlement européen et du Conseil 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*, J. O. des Communautés européennes n° L 281 du 23 octobre 1995 p. 0031-0050.

ORGANISATION DE COOPÉRATION ET DE DÉVELOPPEMENT ÉCONOMIQUES, *Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel*, septembre 1980

CONSEIL DE L'EUROPE, *Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel*, janvier 1981