Ce document constitue un outil de documentation et n'engage pas la responsabilité des institutions

►**B**

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 États-Unis d'Amérique

[notifiée sous le numéro C(2000) 2441]

(Texte présentant de l'intérêt pour l'EEE)

(2000/520/CE)

(JO L 215 du 25.8.2000, p. 7)

Rectifiée par:

►**C1** Rectificatif, JO L 115 du 25.4.2001, p. 14 (2000/520/CE)

▼B

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 États-Unis d'Amérique

[notifiée sous le numéro C(2000) 2441]

(Texte présentant de l'intérêt pour l'EEE)

(2000/520/CE)

LA COMMISSION DES COMMUNAUTÉS EUROPÉENNES,

vu le traité instituant la Communauté européenne,

vu 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 et à la libre circulation de ces données ([1]), et notamment son article 25, paragraphe 6,

considérant ce qui suit:

(1) Conformément à la directive 95/46/CE, les États 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 et si les lois des États membres qui mettent en œuvre d'autres dispositions de la directive sont respectées avant le transfert.

(2) La Commission peut constater qu'un pays tiers assure un niveau de protection adéquat. Dans ce cas, des données à caractère personnel peuvent être transférées sans que des garanties supplémentaires soient nécessaires.

(3) Conformément à la directive 95/46/CE, le niveau de protection des données doit s'apprécier au regard de toutes les circonstances relatives à un transfert ou à une catégorie de transferts de données et compte tenu de conditions données. Le groupe de protection des personnes à l'égard du traitement des données à caractère personnel institué par ladite directive ([2]) a formulé des indications concernant la réalisation de cette évaluation ([3]).

(4) Compte tenu des conceptions différentes de la protection des données dans les pays tiers, l'application du caractère adéquat de cette protection et l'application de toute décision au titre de l'article 25, paragraphe 6, de la directive 95/46/CE doivent se faire d'une façon ne désavantageant de façon arbitraire ou injustifiée aucun des pays tiers où des conditions similaires existent et ne constituent pas un obstacle déguisé aux échanges, eu égard aux engagements internationaux actuels de la Communauté.

(5) Le niveau de protection adéquat pour le transfert de données de la Communauté vers les États-Unis d'Amérique, reconnu conformément à la présente décision, devrait être obtenu si les organisations respectent les «principes de la "sphère de sécurité" relatifs à la protection de la vie privée» (ci-après dénommés «les principes») et les «questions souvent posées» «frequently asked questions» (FAQ) qui fournissent des orientations pour la mise en œuvre des principes publiés par le gouvernement des États-Unis le 21 juillet 2000. En outre, les organisations devraient divulguer

([1]) JO L 281 du 23.11.1995, p. 31.

([2]) Voir adresse: http://www.europa.eu.int/comm/internal_market/en/media/dattaprot/wpdocs/index.htm

([3]) WP 12: «Transferts de données personnelles vers des pays tiers: application des articles 25 et 26 de la directive communautaire sur la protection des données», document adopté le 24 juillet 1998 par le groupe de travail.

▼B

leurs règles de confidentialité et relever de la compétence de la Commission fédérale du commerce [Federal Trade Commission (FTC)] au titre de la section 5 du Federal Trade Commission Act qui interdit les manœuvres et les pratiques déloyales ou frauduleuses dans le domaine du commerce, ou de tout autre organisme officiel assurant efficacement la mise en œuvre des principes conformément aux FAQ.

(6) Les secteurs et/ou les traitements de données qui ne relèvent pas aux États-Unis de la compétence des organes administratifs américains énumérés à l'annexe VII de la présente décision n'entrent pas dans le champ d'application de ladite décision.

(7) Pour que la présente décision soit valablement appliquée, il est nécessaire que les organisations qui souscrivent aux principes et aux FAQ puissent être identifiées par les parties intéressées, telles que les personnes concernées, les exportateurs de données ou les autorités chargées de la protection des données. À cet effet, le ministère américain du commerce, ou son représentant, devrait s'engager à tenir et à rendre publique la liste des organisations qui déclarent leur adhésion aux principes mis en œuvre conformément aux FAQ et qui relèvent de la compétence d'au moins un des organes administratifs énumérés à l'annexe VII de la présente décision.

(8) Dans un souci de transparence et en vue de permettre aux autorités compétentes des États membres d'assurer la protection des individus en ce qui concerne le traitement des données à caractère personnel, il est nécessaire d'indiquer dans la décision dans quelles circonstances exceptionnelles la suspension de certains flux de données peut être justifiée, même si le niveau de protection fourni a été jugé adéquat.

(9) La «sphère de sécurité» créée par les principes et les FAQ peut devoir être revue à la lumière de l'évolution de la protection de la vie privée, dans des circonstances où la technologie rend de plus en plus faciles le transfert et le traitement de données à caractère personnel, ainsi qu'à la lumière de rapports de mise en œuvre élaborés par les autorités compétentes.

(10) Le groupe de protection des personnes à l'égard du traitement des données à caractère personnel, institué en vertu de l'article 29 de la directive 95/46/CE, a formulé des avis sur le niveau de protection assuré par les mesures relatives à la «sphère de sécurité» aux États-Unis, dont il a été tenu compte lors de l'élaboration de la présente décision [1].

(11) Les mesures arrêtées dans la présente décision sont conformes à l'avis du comité institué en vertu de l'article 31 de la directive 95/46/CE.

▼C1

(12) Conformément à la décision 1999/468/CE du Conseil, et notamment à son article 8, le Parlement européen a adopté la

---

[1] WP 15: Avis 1/99 concernant le niveau de protection des données à caractère personnel aux États-Unis et les discussions en cours entre la Commission européenne et le gouvernement américain.
WP 19: Avis 2/99 concernant la pertinence des «principes internationaux de la "sphère de sécurité"» publiés par le ministère du commerce des États-Unis le 19 avril 1999.
WP 21: Avis 4/99 concernant les questions souvent posées, devant être publiées par le ministère américain du commerce dans le cadre des principes proposés pour la «sphère de sécurité».
WP 23: Working document on the current state of play of the ongoing discussions between the European Commission and the United States Government concerning the «International Safe Harbor Principles».
WP 27: Avis 7/99 concernant le niveau de protection des données assuré 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 américain du commerce.
WP 31: Avis 3/2000 concernant le dialogue entre l'Union européenne et les États-Unis sur l'accord relatif à la «sphère de sécurité».
WP 32: Avis 4/2000 concernant le niveau de protection assuré par les «principes de la sphère de sécurité».

▼C1

résolution A5-0177/2000 sur le projet de décision de la Commission relative à la pertinence au niveau de protection fourni par le principe de la sphère de sécurité et par les questions souvent posées y afférentes, publiées par le ministère du commerce des États-Unis d'Amérique [1]. La Commission a réexaminé le projet de décision à la lumière de cette résolution et conclu que, bien que le Parlement européen ait exprimé l'opinion que certaines améliorations devaient être apportées aux principes de la sphère de sécurité et à la FAQ y afférentes avant que l'on puisse considérer qu'une «protection adéquate» est garantie, il n'a pas établi que la Commission dépasserait ses compétences en adoptant la décision,

▼B

A ARRÊTÉ LA PRÉSENTE DÉCISION:

Article premier

1. Aux fins de l'article 25 de la directive 95/46/CE, pour toutes les activités rentrant dans le domaine d'application de ladite directive, il est considéré que les «principes de la "sphère de sécurité" relatifs à la protection de la vie privée» (ci-après dénommés «les principes visés à l'annexe I de la présente décision»), appliqués conformément aux orientations fournies par les «questions souvent posées» [«frequently asked questions» (FAQ)] publiées le 21 juillet 2000 par le ministère du commerce des États-Unis d'Amérique, visées à l'annexe II de la présente décision, assurent un niveau adéquat de protection des données à caractère personnel transférées depuis la Communauté vers des organisations établies aux États-Unis compte tenu des documents suivants émis par le ministère du commerce des États-Unis:

a) une étude relative à la mise en œuvre des principes de la sphère de sécurité, visée à l'annexe III;

b) un aide-mémoire sur la réparation des préjudices subis par suite d'atteintes à la vie privée et sur les autorisations explicites prévues par le droit américain, visé à l'annexe IV;

c) une lettre de la Commission fédérale du commerce, visée à l'annexe V;

d) une lettre du ministère des transports des États-Unis, visée à l'annexe VI.

2. En ce qui concerne chaque transfert de données, les conditions suivantes doivent être remplies:

a) l'organisation destinataire des données s'est clairement et publiquement engagée à observer les principes mis en œuvre conformément aux FAQ et

b) l'organisation est soumise aux pouvoirs légaux d'un organe administratif américain énuméré à l'annexe VII de la présente décision, habilité à instruire des plaintes et à obtenir des mesures de redressement contre les pratiques déloyales ou frauduleuses ainsi que la réparation des préjudices subis par les personnes concernées, quel que soit leur pays de résidence ou leur nationalité, en cas de non-respect des principes mis en œuvre conformément aux FAQ.

3. Les conditions indiquées au paragraphe 2 sont considérées comme remplies par chaque organisation qui a déclaré son adhésion aux principes mis en œuvre conformément aux FAQ à compter de la date à laquelle elle avise le ministère américain du commerce (ou son représentant) de la divulgation de l'engagement visé au paragraphe 2, point a), et de l'identité de l'organe administratif visé au paragraphe 2, point b).

[1] La résolution n'a pas encore été publiée au Journal officiel.

▼B

Article 2

La présente décision concerne uniquement le caractère adéquat de la protection fournie aux États-Unis par les principes mis en œuvre conformément aux FAQ en vue de répondre aux exigences de l'article 25, paragraphe 1, de la directive 95/46/CE et n'affecte pas l'application d'autres dispositions de ladite directive qui se rapportent au traitement de données à caractère personnel dans les États membres, et notamment de son article 4.

Article 3

1. Sans préjudice de leurs pouvoirs de prendre des mesures visant à assurer le respect des dispositions nationales adoptées en application de dispositions autres que celles de l'article 25 de la directive 95/46/CE, les autorités compétentes des États membres peuvent exercer les pouvoirs dont elles disposent pour suspendre les flux de données vers une organisation adhérant aux principes mis en œuvre conformément aux FAQ afin de protéger les individus en ce qui concerne le traitement de leurs données personnelles, et ce dans les cas:

a) où l'organe administratif américain visé à l'annexe VII de la présente décision, ou une instance indépendante de recours au sens du point a) du principe d'application visé à l'annexe I de la présente décision, a constaté que l'organisation viole les principes mis en œuvre conformément aux FAQ ou

b) où il est fort probable que les principes sont violés; où il y a tout lieu de croire que l'instance d'application concernée ne prend pas ou ne prendra pas en temps voulu les mesures qui s'imposent en vue de régler l'affaire en question; où la poursuite du transfert ferait courir aux personnes concernées un risque imminent de subir des dommages graves; et où les autorités compétentes des États membres se sont raisonnablement efforcées, compte tenu des circonstances, d'avertir l'organisation et de lui donner la possibilité de répondre.

La suspension cesse dès que le respect des principes mis en œuvre conformément aux FAQ est assuré et que les autorités compétentes de la Communauté en sont avisées.

2. Les États membres informent sans tarder la Commission de l'adoption de mesures fondées sur le paragraphe 1.

3. Les États membres et la Commission s'informent aussi mutuellement des cas dans lesquels les organismes chargés de faire respecter les principes mis en œuvre conformément aux FAQ aux États-Unis ne parviennent pas à s'acquitter de leur tâche.

4. Si les informations recueillies en application des paragraphes 1, 2 et 3 montrent qu'un quelconque organisme chargé de faire respecter les principes mis en œuvre conformément aux FAQ aux États-Unis ne remplit pas efficacement sa mission, la Commission informe le ministère américain du commerce et, si nécessaire, propose un projet des mesures à prendre, conformément à la procédure visée à l'article 31 de la directive 95/46/CE, en vue d'abroger ou de suspendre la présente décision ou d'en limiter la portée.

Article 4

1. La présente décision peut être adaptée à tout moment à la lumière de l'expérience acquise durant sa mise en œuvre et/ou si le niveau de protection assuré par les principes et les FAQ est dépassé par les exigences du droit américain. La Commission évalue, en tout état de cause, l'application de la présente décision, sur la base des informations disponibles, trois ans après sa notification aux États membres et communique au comité institué au titre de l'article 31 de la directive 95/46/CE toute constatation pertinente, y compris tout élément susceptible d'influer sur l'évaluation selon laquelle les dispositions de

▼B

l'article 1er de la présente décision assurent un niveau de protection adéquat au sens de l'article 25 de la directive 95/46/CE et toute information montrant que la présente décision est appliquée de manière discriminatoire.

2. La Commission présente, si nécessaire, un projet des mesures à prendre conformément à la procédure visée à l'article 31 de la directive 95/46/CE.

Article 5

Les États membres prennent toutes les mesures nécessaires pour se conformer à la présente décision au plus tard quatre-vingt-dix jours après la date de sa notification aux États membres.

Article 6

Les États membres sont destinataires de la présente décision.

▼B

ANNEXE I

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

La directive européenne sur la protection des données, qui constitue un cadre législatif détaillé en matière de protection de la vie privée, est entrée en vigueur le 25 obtobre 1998. Elle stipule que des données à caractère personnel ne peuvent être tranférées que vers des pays tiers assurant un niveau de protection adéquat. Même si les États-Unis et l'Union européenne ont comme objectif commun de protéger davantage la vie privée de leurs citoyens, les États-Unis préconisent dans ce domaine une approche différente de celle de l'Union européenne. Ils se basent, en effet, sur un système sectoriel qui fait appel à un ensemble disparate de dispositions législatives et réglementaires ainsi qu'à des codes d'autoréglementation. Compte tenu de ces différences, de nombreuses organisations américaines ont fait part de leur incertitude quant à l'incidence d'un «niveau de protection adéquat» sur les transferts de données à caractère personnel de l'Union européenne vers les États-Unis.

Pour réduire cette incertitude et pour fournir un cadre plus clair en vue de tels transferts, le ministère américain du commerce publie le présent document («les principes») ainsi que les «questions souvent posées» (FAQ) en vertu de son autorité légale afin de stimuler, de promouvoir et de développer le commerce international. Les principes ont été élaborés en concertation avec les entreprises et le grand public dans le but de faciliter le commerce et les relations d'affaires entre les États-Unis et l'Union européenne. Ils sont exclusivement destinés aux organisations américaines recevant des données à caractère personnel en provenance de l'Union européenne et doivent permettre à ces organisations de remplir les conditions relatives à la «sphère de sécurité» de façon à bénéficier de la présomption de «niveau de protection adéquat» que prévoit celle-ci. Comme les principes n'ont été conçus que pour servir cet objectif spécifique, leur adoption à d'autres fins peut s'avérer inadéquate. Les principes ne peuvent pas se substituer aux dispositions nationales de mise en œuvre de la directive qui sont applicables au traitement des données à caractère personnel dans les États membres.

Toute organisation est libre de remplir ou non les conditions relatives à la «sphère de sécurité» et dispose de plusieurs moyens pour s'y conformer. Les organisations qui décident d'adhérer aux principes doivent les respecter pour obtenir et conserver les avantages de la «sphère de sécurité» et doivent annoncer publiquement leur décision. Si, par exemple, une organisation participe à un programme sur la protection de la confidentialité géré par le secteur privé qui respecte ces principes, elle remplit lesdites conditions. Une organisation peut également intégrer la «sphère de sécurité» en mettant au point ses propres règles en matière de protection des données, pour autant que celles-ci soient conformes auxdits principes. Toute organisation qui a opté pour l'une de ces deux solutions et qui enfreint les principes doit être sanctionnée conformément à la section 5 du Federal Trade Commission Act, qui interdit les pratiques déloyales ou frauduleuses, ou à toute autre loi du même type (voir, en annexe, la liste des instances réglementaires américaines reconnues par l'Union européenne). En outre, lorsqu'une organisation est soumise à un ensemble de dispositions juridiques, réglementaires, administratives ou autres (ou encore à un ensemble de règles) qui assurent une protection efficace des données à caractère personnel, elle peut également bénéficier des avantages de la «sphère de sécurité». Dans tous les cas, l'organisation bénéficie desdits avantages à compter de la date à laquelle elle avise le ministère du commerce (ou la personne désignée par celui-ci) de son adhésion aux principes, conformément aux recommandations énoncées dans la FAQ relative à l'autocertification.

L'adhésion aux principes peut être limitée par: a) les exigences relatives à la sécurité nationale, l'intérêt public et le respect des lois des États-Unis; b) les textes législatifs, les règlements administratifs ou les décisions jurisprudentielles qui créent des obligations contradictoires ou prévoient des autorisations explicites, pour autant qu'une organisation qui a recours à une telle autorisation peut démontrer que le non-respect des principes est limité aux mesures nécessaires pour garantir les intérêts légitimes supérieurs que cette autorisation vise à servir; c) les exceptions ou les dérogations prévues par la directive ou par le droit national, à condition que ces exceptions ou dérogations soient appliquées dans des contextes comparables. Conformément à l'objectif d'un renforcement de la protection de la vie privée, les organisations doivent s'efforcer d'appliquer ces principes de manière complète et transparente, y compris en indiquant — dans leurs codes de protection de la vie privée — dans quels domaines les exceptions visées au point b) ci-dessus s'appliqueront de façon régulière. Pour la même raison, lorsque les principes et/ou les lois des États-Unis permettent aux organisations de faire un choix, celles-ci sont invitées à opter, dans la mesure du possible, pour le niveau de protection le plus élevé.

▼B

Pour des raisons d'ordre pratique ou autres, certaines organisations souhaiteront peut-être appliquer les principes à l'ensemble de leurs données, mais elles ne sont tenues de le faire que pour les données tranférées ultérieurement à leur adhésion à la «sphère de sécurité». Pour intégrer celle-ci, il n'est pas nécessaire d'appliquer les principes aux données traitées manuellement. Les organisations qui souhaitent bénéficier des avantages de la «sphère de sécurité» pour accéder à des données provenant de fichiers de l'Union européenne traités manuellement doivent appliquer les principes à toute information transférée après leur adhésion auxdits principes. Les organisations qui désirent étendre les avantages de la «sphère de sécurité» à des informations personnelles tirées de fichiers de type «ressources humaines» en provenance de l'Union européenne afin de les utiliser dans le cadre d'une relation de travail doivent mentionner cette intentionlorsqu'elles autocertifient leur engagement auprès du ministère américain du commerce (ou auprès de la personne désignée par celui-ci) et doivent se conformer aux exigences exposées dans la FAQ sur l'autocertification. Les organisations pourront également mettre en place les garanties visées à l'article 26 de la directive si elles appliquent les principes — dans le cadre d'accords écrits avec des parties transférant des données depuis l'Union européenne — aux dispositions normatives concernant la protection de la vie privée, une fois que les autres dispositions relatives à ces contrats types auront été approuvées par la Commission et les États membres.

Le droit américain est applicable en ce qui concerne l'interprétation et le respect des principes de la «sphère de sécurité» (y compris les questions souvent posées) et des mesures de protection de la vie privée mise en œuvre par les organisations adhérant à la «sphère de sécurité», à l'exception des cas dans lesquels des organisations se sont engagées à coopérer avec les autorités européennes chargées de la protection des données. Sauf indication contraire, toutes les dispositions de la «sphère de sécurité» et des questions souvent posées sont applicables.

Par «donnée ou information à caractère personnel», il faut entendre toute donnée ou information concernant une personne identifiée ou identifiable qui entre dans le champ d'application de la directive, qui est transférée de l'Union européenne vers une organisation américaine et qui est enregistrée sous quelque forme que ce soit.

NOTIFICATION

Toute organisation doit informer les personnes concernées des raisons de la collecte et de l'utilisation d'informations à caractère personnel, de la façon de la contacter pour toute demande ou plainte, des tiers auxquels les informations sont communiquées, des choix et des moyens qu'offre l'organisation aux personnes concernées pour limiter l'utilisation et la divulgation de ces données. La notification doit être établie dans un langage clair et bien lisible. Elle doit être communiquée aux personnes concernées lorsque celles-ci sont invitées pour la première fois à fournir des informations à caractère personnel ou dès que possible après cette invitation et, en tout état de cause, 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 ([1]).

CHOIX

Toute organisation doit offrir aux personnes concernées la possibilité de décider (opposition) si leurs informations à caractère prsonnel a) peuvent être divulguées à une tierce personne ([1]) ou b) peuvent être utilisées dans un but incompatible avec le ou les objectifs pour lesquels les données ont été initialement collectées ou dans un but approuvé ultérieurement par la personne concernée. Les personnes concernées doivent disposer de mécanismes clairs et visibles, d'accès facile et d'un coût raisonnable pour opérer leur choix.

En ce qui concerne les informations sensibles (par exemple, les données concernant le dossier médical ou l'état de santé d'une personne, son origine raciale ou ethnique, ses opinions politiques, ses croyances religieuses ou ses convictions philosophiques, son affiliation à un syndicat ou sa sexualité), toute personne doit avoir positivement ou explicitement la possibilité de décider (consentement) si les données peuvent être divulguées à un 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. En tout état de cause, une organisation considérera comme sensible toute information reçue d'un tiers si le tiers indique que cette information est sensible et la traite en conséquence.

([1]) Il n'est pas nécessaire de procéder à une notification ou à un choix quand des données sont communiquées à un tiers qui est chargé d'effectuer des travaux pour le compte et selon les instructions de l'organisation. En revanche, le principe du transfert ultérieur est applicable à de semblables communications.

▼B

TRANSFERT ULTÉRIEUR

Pour divulguer des informations à un tiers, les organisations sont tenues d'appliquer les principes de notification et de choix. Les organisations qui le souhaitent peuvent transférer des informations à un tiers agissant en qualité de mandataire, conformément à la description fournie dans la note finale, si elles certifient auparavant que le tiers 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 encore si elle passe un accord écrit avec ce tiers dans lequel celui-ci s'engage à assurer au moins le même niveau de protection que les principes. Si l'organisation se conforme aux exigences susmentionnées, elle ne sera pas passible de poursuites (sauf accord contraire de sa part) dans les cas où un tiers auquel elle aura transféré de telles données traitera celles-ci d'une façon contraire aux dispositions ou aux restrictions convenues, sauf si l'organisation savait ou aurait dû savoir que le tiers traiterait les données de cette manière et que l'organisation n'a pas pris de mesures appropriées pour prévenir ce traitement ou y mettre fin.

SÉCURITÉ

Les organisations qui créent, gèrent, utilisent ou diffusent des données à caractère personnel doivent prendre les mesures nécessaires pour éviter la perte, l'utilisation abusive, la consultation illicite, la divulgation, la modification et la destruction de ces données.

INTÉGRITÉ DES DONNÉES

Compte tenu de ces principes, les informations à caractère personnel doivent être pertinentes pour les utilisations auxquelles elles sont destinées. Une organisation ne peut pas traiter des données à caractère personnel d'une manière qui est incompatible avec les objectifs pour lesquels elles ont été collectées ou avec les objectifs approuvés ultérieurement par la personne concernée. Toute organisation doit donc prendre les mesures qui s'imposent, dans la limite de ces objectifs, pour assurer la fiabilité des données par rapport à l'utilisation prévue ainsi que leur exactitude, leur exhaustivité et leur actualité.

ACCÈS

Lorsqu'une organisation détient des informations à caractère personnel sur une personne, celle-ci doit avoir accès à ces données et doit pouvoir les corriger, les modifier ou les supprimer lorsqu'elles sont inexactes. Font toutefois exception à cette règle les cas où la charge de travail ou la dépense qu'occasionnerait le droit d'accès sont disproportionnées par rapport aux risques pesant sur la vie privée de la personne concernée ainsi que les cas susceptibles d'entraîner une violation des droits d'autres personnes.

MISE EN ŒUVRE

Pour protéger efficacement la vie privée, il convient notamment de mettre au point des mécanismes permettant d'assurer le respect des principes de la «sphère de sécurité», de ménager un droit de recours aux personnes concernées par le non-respect des principes et de sanctionner les organisations qui n'ont pas appliqué les principes alors qu'elles s'y sont engagées. Ces mécanismes doivent comprendre au minimum: a) des systèmes de recours indépendants, aisément accessibles et peu coûteux, permettant d'étudier et de résoudre toute plainte et tout litige en se référant aux principes et d'accorder des dédommagements lorsque la loi applicable ou les initiatives du secteur privé le prévoient; b) des procédures de suivi permettant de vérifier que les renseignements et les indications fournies par les entreprises sur leurs pratiques en matière de protection de la vie privée sont exactes et que ces pratiques sont mises en œuvre conformément aux déclarations des entreprises; c) des déclarations faisant obligation aux organisations qui souscrivent aux principes de résoudre les problèmes résultant du non-respect de ceux-ci et prévoyant des sanctions pour les contrevenants. Ces sanctions doivent être suffisamment dissuasives pour garantir le respect des principes.

▼B

Annexe

Liste des organismes officiels des États-Unis reconnus par l'Union européenne

L'Union européenne reconnaît les organismes gouvernementaux des États-Unis suivants comme étant autorisés à examiner des plaintes et à bénéficier d'une assistance contre des pratiques déloyales, de même qu'en matière de réparation pour des personnes en cas de non-conformité aux principes en vigueur conformément aux FAQ:

— la Federal Trade Commission, sur la base des pouvoirs qui lui sont conférés en vertu de la section 5 du Federal Trade Commission Act,

— le Department of Transportation, sur la base des pouvoirs qui lui sont conférés en vertu du titre 49 du United States Code, section 41712.

▼B

ANNEXE II

QUESTIONS SOUVENT POSÉES (FAQ)

FAQ 1 — Données sensibles

Q: *Une organisation doit-elle toujours fournir un choix explicite (opt in) en ce qui concerne les données sensibles?*

R: Non, un tel choix n'est pas requis lorsque le traitement est: 1) dans l'intérêt vital de la personne concernée ou d'une autre personne; 2) nécessaire à la constatation d'un droit ou d'une défense en justice; 3) nécessaire pour dispenser des soins médicaux à des fins de diagnostic; 4) effectué au cours d'activités légitimes par une fondation, une association ou tout autre organisme à but non lucratif et à finalité politique, philosophique, religieuse ou syndicale, et à condition que le traitement se rapporte aux seuls membres de l'organisme ou aux personnes entretenant avec lui des contacts réguliers liés à sa finalité et que les données ne soient pas communiquées à des tiers sans le consentement des personnes concernées; 5) nécessaire aux fins de respecter les obligations de l'organisation en matière de droit du travail; 6) lié à des données manifestement rendues publiques par l'individu.

FAQ 2 — Exceptions journalistiques

Q: *Compte tenu des garanties qu'offre la Constitution américaine en ce qui concerne la liberté de la presse et de l'exemption prévue dans la directive pour les informations utilisées par les journalistes, les principes de la «sphère de sécurité» s'appliquent-ils aux informations à caractère personnel recueillies pour les besoins de la presse?*

R: Lorsque les droits de la presse visés dans le premier amendement à la Constitution des États-Unis ne sont pas compatibles avec la protection de la vie privée, le premier amendement doit primer pour les activités qui sont le fait de personnes ou d'organisations américaines. Les informations personnelles qui sont recueillies à des fins de publication, de diffusion ou d'autres formes de communication publique, qu'elles soient utilisées ou non, ainsi que les informations qui ont été publiées antérieurement, puis archivées ne sont pas soumises aux principes de la «sphère de sécurité»

FAQ 3 — Responsabilité secondaire

Q: *Les fournisseurs d'accès Internet (FAI), les sociétés de télécommunications et d'autres organismes sont-ils soumis aux principes de la «sphère de sécurité» lorsqu'ils se limitent à transmettre, acheminer, remplacer ou masquer, pour le compte d'un autre organisme, des informations susceptibles de violer ces principes?*

R: Non. Pas plus que la directive elle-même, la «sphère de sécurité» ne fait naître de responsabilité secondaire. Dans la mesure où un organisme sert uniquement de vecteur à des données transmises par des tiers et ne détermine ni les buts ni les moyens de traitement de ces données à caractère personnel, sa responsabilité ne peut être engagée.

FAQ 4 — Banques d'investissement et audits

Q: *Les activités des commissaires aux comptes et des banques d'investissement peuvent impliquer le traitement de données à caractère personnel sans l'assentiment ou à l'insu de la personne concernée. Dans quelles circonstances les principes de notification, de choix et d'accès l'autorisent-ils?*

R: Les banques d'investissement et les commissaires aux comptes peuvent traiter des informations à l'insu de la personne concernée, uniquement dans la mesure et pendant la durée nécessaires pour satisfaire à des dispositions réglementaires ou à des exigences liées à l'intérêt général ainsi que dans d'autres circonstances où l'application de ces principes porterait atteinte aux intérêts légitimes de l'organisme. Parmi ces intérêts légitimes figurent la surveillance du respect, par les entreprises, de leurs obligations légales et de leurs activités comptables légitimes ainsi que la confidentialité qui doit être observée dans le contexte d'éventuelles acquisitions, fusions, coentreprises ou d'autres transactions de nature

▼B

comparable effectuées par les banques d'investissement ou les commissaires aux comptes.

FAQ 5 [1] **— Rôle des autorités chargées de la protection des données**

Q: *Par quels moyens les entreprises qui le souhaitent prendront-elles l'engagement de coopérer avec les autorités de l'Union européenne chargées de la protection des données (DPA) et comment ces engagements seront-ils appliqués?*

R: Dans le cadre de la «sphère de sécurité», les organisations américaines recevant des données à caractère personnel en provenance de l'Union européenne doivent s'engager à utiliser des mécanismes efficaces assurant le respect des principes de la «sphère de sécurité». Plus précisément, comme le prévoit le principe d'application, ces mécanismes doivent prévoir: a) des voies de recours pour les personnes auxquelles les données se réfèrent, b) des procédures de suivi permettant de contrôler la véracité des affirmations et des déclarations faites par les organisations en ce qui concerne le respect de la vie privée et c) des dispositions aux termes desquelles les organisations sont tenues de résoudre les problèmes qui découlent du non-respect des principes et d'assumer les conséquences qui en résultent. Une organisation est tenue de satisfaire aux points a) et c) du principe d'application si elle souscrit à l'engagement de coopération avec les DPA visé à la présente FAQ.

Une organisation peut s'engager à coopérer avec les DPA en déclarant dans sa certification d'adhésion à la «sphère de sécurité» adressée au ministère du commerce (voir FAQ 6 relative à l'autocertification) que l'organisation:

1) décide de se conformer aux dispositions des points a) et c) du principe d'application de la «sphère de sécurité» en s'engageant à coopérer avec les DPA;

2) coopérera avec les DPA au niveau de l'instruction et du règlement des plaintes déposées au titre de la «sphère de sécurité»;

3) suivra tout avis donné par les DPA selon lequel l'organisation devra prendre des mesures spécifiques pour respecter les principes de la «sphère de sécurité», y compris toute mesure de réparation ou d'indemnisation au bénéfice des particuliers qui ont subi un préjudice en raison du non-respect desdits principes, et informera par écrit les DPA des mesures prises à cet effet.

La coopération des DPA se traduira par des informations et des avis donnés selon les modalités suivantes:

— les DPA seront consultées par l'intermédiaire d'un *panel* informel des DPA établi au niveau européen qui, notamment, contribuera à définir une approche harmonisée et cohérente,

— le *panel* conseillera les organisations américaines concernées au sujet de plaintes non résolues de particuliers portant sur le traitement des informations personnelles qui ont été transférées au départ de l'Union européenne au titre de la «sphère de sécurité». Les conseils donnés viseront à assurer une application correcte des principes de la «sphère de sécurité» et porteront également sur les mécanismes de règlement des litiges que les DPA jugeront appropriés pour le ou les particuliers concernés,

— le *panel* donnera son avis en réponse aux recours formés par les organisations concernées et/ou aux plaintes introduites directement par des particuliers contre des organisations qui se sont engagées à coopérer avec les DPA aux fins du respect des principes de la «sphère de sécurité», tout en encourageant et, le cas échéant, en aidant ces particuliers à faire d'abord usage des mécanismes internes d'instruction des plaintes dont l'organisation dispose,

— l'avis ne sera donné qu'après avoir mis les deux parties en mesure de présenter leurs observations et, le cas échéant, de produire leurs moyens de preuve. Le *panel* veillera à donner son avis dans les meilleurs délais tout en respectant les principes du procès équitable.

[1] L'inclusion de cette FAQ dans l'accord est subordonnée à l'assentiment des DPA. Celles-ci ont examiné le présent texte au sein du groupe de travail de l'article 29 et la plupart d'entre elles l'ont jugée acceptable, mais elles ne sont disposées à se prononcer définitivement que dans le contexte de l'avis global que le groupe de travail mettra au sujet de l'accord définitif.

▼B

En principe, le *panel* se prononcera au plus tartd dans un délai de soixante jours à compter de la réception de la plainte ou du recours,

— s'il le juge approprié, le *panel* rendra publics les résultats de l'examen des plaintes dont il a été saisi,

— l'avis du *panel* n'engage ni le *panel* ni les DPA qui le composent.

Les organisations optant pour ce mode de règlement des litiges devront s'engager à se conformer aux avis émis par les DPA. Si une organisation ne s'exécute par dans un délai de vingt-cinq jours à compter de la notification de l'avis sans pouvoir fournir de motif valable, le *panel* pourra décider de soumettre l'affaire à la Federal Trade Commission ou à une autre instance réglementaire américaine visée à l'annexe des principes de la «sphère de sécurité» ou de conclure à un manquement grave à l'engagement de coopérer, lequel devra, en conséquence, être considéré comme nul et non avenu. Dans le dernier cas, le *panel* informera le ministère du commerce (ou son représentant) afin que celui-ci corrige la liste des adhérents à la «sphère de sécurité». Tout manquement à l'engagement de coopérer avec le *panel* ainsi que tout non-respect des principes de la «sphère de sécurité» seront considérés comme constitutifs d'un acte frauduleux au titre de la section 5 de la loi instituant la Federal Trade Commission ou de lois équivalentes.

Les organisations optant pour cette formule devront verser une cotisation annuelle couvrant les frais de gestion du *panel* et seront, le cas échéant, invitées à participer aux frais de traduction résultant de l'examen, par le *panel* , des recours formés et des plaintes déposées contre elles. La cotisation annuelle n'excédera pas 500 dollars des États-Unis et sera réduite pour les petites entreprises.

La possibilité de coopérer avec les DPA sera ouverte aux organisations adhérant à la «sphère de sécurité» au cours d'une période de trois ans. Les DPA réviseront les dispositions avant la fin de cette période si le nombre d'organisations américaines optant pour cette formule était excessif.

FAQ 6 — Autocertification

Q: *Comment une organisation autocertifie-t-elle qu'elle adhère aux principes de la «sphère de sécurité»?*

R: Les avantages afférents à la «sphère de sécurité» sont acquis à partir de la date à laquelle une organisation autocertifie au ministère américain du commerce (ou à la personne désignée par celui-ci) qu'elle adhère aux principes conformément aux modalités ci-dessous.

Pour autocertifier son adhésion à la «sphère de sécurité», une organisation peut remettre au ministère américain du commerce (ou à la personne désignée par celui-ci) une lettre signée d'un cadre de ladite organisation contenant 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 (et qui est mentionnée dans l'annexe aux principes); 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) ([1]) et g) l'instance de recours indépendante qui pourra instruire les plaintes non résolues.

Une organisation peut étendre les avantages de la «sphère de sécurité» à des informations de type «ressources humaines» qui sont transférées depuis l'Union européenne afin d'être utilisées dans le cadre de relations de travail, lorsque l'une des instances réglementaires mentionnées dans

([1]) Voir la FAQ 7 sur la vérification.

▼B

l'annexe aux principes est compétente pour statuer sur les plaintes déposées, le cas échéant, contre ladite organisation dans le domaine des informations de type «ressources humaines». En outre, l'organisation doit indiquer dans sa lettre d'autocertification qu'elle désire couvrir de telles informations, qu'elle s'engage à coopérer avec les autorités compétentes de l'Union européenne conformément aux termes des FAQ 5 et 9 et qu'elle observera les conseils donnés par ces autorités.

Le ministère (ou la personne désignée par celui-ci) tiendra une liste de l'ensemble des organisations qui suivent cette procédure, garantissant ainsi les avantages de la «sphère de sécurité», et mettra à jour cette liste sur la base des lettres et notifications reçues chaque année en conformité avec la FAQ 11. Ces lettres d'autocertification seront envoyées au moins une fois par an, à défaut de quoi l'organisation sera rayée de la liste et les avantages de la«sphère de sécurité» ne lui seront plus acquis. La liste et les lettres d'autocertification présentées par les organisations seront rendues publiques. Toute organisation qui autocertifie son adhésion aux principes de la «sphère de sécurité» doit également mentionner, dans ses déclarations publiques relatives à sa politique en matière de protection de la vie privée, qu'elle adhère aux principes de la «sphère de sécurité».

L'engagement d'adhérer aux principes n'est pas limité dans le temps en ce qui concerne les données reçues au cours de la période durant laquelle l'organisation bénéficie des avantages de la «sphère de sécurité». Son engagement signifie qu'elle continuera à appliquer les principes à ces données aussi longtemps qu'elle stockera, utilisera ou divulguera celles-ci, même si elle quitte ultérieurement la «sphère de sécurité» pour quelque raison que ce soit.

Lorsqu'une organisation cesse d'exister en tant qu'entité juridique distincte en raison d'une opération de fusion ou d'absorption, elle doit le notifier à l'avance au ministère du commerce (ou à la personne désignée par celui-ci). La notification doit également indiquer si l'entité qui l'absorbe ou l'entité qui naît de la fusion 1) reste soumise aux principes de la «sphère de sécurité» en vertu des dispositions juridiques régissant la fusion ou l'absorption ou 2) si elle choisit d'autocertifier son adhésion aux principes de la «sphère de sécurité» ou de mettre en place d'autres garanties telles qu'un accord écrit certifiant l'adhésion à ces principes. Si aucune des solutions visées aux points 1) et 2) n'est mise en œuvre, toute donnée acquise dans le cadre de la «sphère de sécurité» doit être effacée sans tarder.

Une organisation n'est pas tenue de soumettre toutes les informations personnelles aux principes de la «sphère de sécurité», mais elle doit y soumettre l'ensemble des données personnelles reçues en provenance de l'Union européenne après son adhésion à la «sphère de sécurité».

Toute fausse déclaration au grand public concernant l'adhésion d'une organisation aux principes de la «sphère de sécurité» peut donner lieu à des poursuites devant la Commission fédérale du commerce ou devant toute autre instance administrative compétente. Toute fausse déclaration au ministère du commerce (ou à la personne désignée par celui-ci) peut donner lieu à des poursuites au titre de la loi sur les fausses déclarations (18 USC, article 1001).

FAQ 7 — Vérification

Q: *Quelles sont les pratiques de suivi utilisées par les organisations pour vérifier que les attestations et les déclarations des entreprises sur leurs pratiques en matière de protection de la vie privée en «sphère de sécurité» sont sincères et que ces pratiques ont été mises en œuvre conformément à leurs déclarations et aux principes de la «sphère de sécurité»?*

R: Pour répondre aux exigences de vérification du principe de mise en vigueur, une organisation peut vérifier de telles attestations et déclarations en organisant une autoévaluation ou un contrôle extérieur de la conformité.

Dans le cadre de l'autoévaluation, la vérification devrait établir que la politique en matière de protection de la vie privée, en ce qui concerne les informations personnelles reçues de l'Union européenne, qui est rendue publique par l'organisation, est appropriée, complète, affichée de façon bien visible, totalement mise en œuvre et accessible. Elle devrait aussi montrer que cette politique est conforme aux principes de la «sphère de sécurité», que les personnes sont informées de l'existence de mécanismes internes de traitement des réclamations et des mécanismes indépendants par le truchement desquels ils peuvent diligenter leur plaintes, que l'organisation dispose de procédures de formation des salariés à cet effet et que des sanctions leur sont infligées s'ils ne les respectent pas, et qu'il existe des procédures internes visant à contrôler régulièrement et

▼B

objectivement la conformité avec ce qui précède. Une déclaration vérifiant l'autoévaluation doit être signée au moins une fois par an par un responsable de la société ou tout autre représentant mandaté et transmise à la demande des personnes concernées ou dans le cadre d'une enquête ou d'une réclamation pour non-conformité.

Les organisations doivent conserver des archives sur la mise en œuvre de leurs pratiques relatives à la protection de la vie privée en «sphère de sécurité» et remettre celles-ci sur demande, dans le cadre d'une enquête ou d'une réclamation pour non-conformité, à l'organisme indépendant responsable de l'examen des réclamations ou à l'agence compétente en matière de pratiques déloyales et frauduleuses.

Si l'organisation opte pour un contrôle extérieur de la conformité, ce dernier devra démontrer que la politique de l'organisation en matière de protection de la vie privée, en ce qui concerne les informations reçues de l'Union européenne, respecte les principes de la «sphère de sécurité», que cette politique est respectée et que les particuliers sont informés des mécanismes leur permettant d'introduire des réclamations. Les méthodes utilisées sont diverses. Il peut s'agir (liste non exhaustive) d'un audit, d'une vérification menée de façon aléatoire, de l'utilisation de «leurres» oud'outils technologiques. Une déclaration confirmant qu'un contrôle extérieur de la conformité a été mené à bien doit être signée au moins une fois par an par le contrôleur, le responsable de la société ou tout autre représentant mandaté et transmise à la demande des personnes concernées ou dans le cadre d'une enquête ou d'une réclamation pour non-conformité.

FAQ 8 — Accès

Principe de l'accès

Toute personne doit pouvoir accéder aux informations qu'une organisation détient à son sujet et disposer du droit de corriger, de modifier ou de supprimer ces informations lorsqu'elles sont inexactes, pour autant que cet accès n'entraîne pas une charge ou des coûts disproportionnés par rapport aux risques pour la protection de la vie privée de la personne concernée et qu'il n'y ait pas violation des droits légitimes de tiers.

Q 1: *Le droit d'accès est-il absolu?*

R 1: Non. Conformément aux principes de la «sphère de sécurité», le droit d'accès est un élément fondamental de la protection de la vie privée. Il permet, notamment, à chaque personne de vérifier l'exactitude des informations la concernant. Néanmoins, l'obligation qui incombe à une organisation de donner l'accès aux informations personnelles qu'elle détient dépend du principe de la proportionnalité ou du caractère raisonnable de la demande de l'accès et, dans certains cas, elle doit être modulée. En effet, l'exposé des motifs des lignes directrices de l'Organisation de coopération et de développement économique (OCDE) sur la protection de la vie privée (1980) indique clairement que l'obligation pour une organisation de fournir un accès n'est pas absolue. Le droit d'accès n'exige pas des recherches aussi approfondies que pour une citation à comparaître, par exemple, pas plus que l'accès à toutes les formes de stockage de données par l'organisation.

L'expérience a plutôt montré que, lorsqu'elle répond aux demandes d'accès individuelles, l'organisation doit avant tout être guidée par la ou les motivations de leur auteur. Par exemple, si une demande d'accès est vague ou a une portée très large, l'organisation peut engager un dialogue avec le demandeur afin de mieux comprendre sa démarche et de trouver les informations appropriées. L'organisation peut chercher à déterminer avec quels services la personne concernée a eu des contacts et/ou quelle est la nature (ou l'utilisation) des informations qui font l'objet de la demande d'accès. Cependant, personne ne doit justifier une demande d'accès à ses propres données.

Les coûts et la charge constituent des facteurs importants qui sont à prendre en compte, mais qui ne sont pas décisifs lorsqu'il s'agit de déterminer le caractère raisonnable de l'accès. Ainsi, conformément aux autres dispositions des présentes FAQ, si les informations sont utilisées pour prendre des décisions qui auront des conséquences majeures pour la personne (par exemple, le refus ou l'octroi d'avantages importants, tels qu'une assurance, une hypothèque ou un emploi), l'organisation est tenue de les communiquer, même si cela s'avère relativement difficile ou coûteux.

Lorsque les informations demandées ne sont pas sensibles ou ne sont pas utilisées pour prendre des décisions qui auront des conséquences majeures

▼B

pour la personne (par exemple, les données de *marketing* non sensibles qui sont utilisées pour l'envoi de catalogues), mais qu'elles sont aisément disponibles et que leur transmission est peu coûteuse, l'organisation est tenue de permettre à toute personne qui en fait la demande d'accéder aux informations factuelles qui la concernent. Ces informations peuvent comporter des éléments obtenus auprès de la personne elle-même, recueillis lors d'une transaction ou transmis par des tiers qui ont un lien avec la personne concernée.

Le droit d'accès étant par nature un élément fondamental de la protection de la vie privée, les organisations doivent, toujours et en toute bonne foi, faire des efforts pour fournir l'accès. Par exemple, s'il convient de protéger certaines informations et que celles-ci peuvent être aisément séparées des informations qui font l'objet d'une demande d'accès, l'organisation doit procéder à la séparation des données confidentielles et répondre à la demande en rendant les autres informations disponibles. Si l'organisation décide de refuser l'accès dans un cas précis, elle doit motiver sa décision et communiquer les coordonnées d'une personne à contacter pour plus d'informations.

Q 2: *Qu'est-ce qu'une information commerciale confidentielle et les organisations sont-elles autorisées à en refuser l'accès pour des raisons de sauvegarde?*

R 2: Les informations commerciales confidentielles (telles qu'elles sont désignées dans le code de procédure fédéral sur la communication de données) sont des informations qu'une organisation veille à ne pas divulguer car elles favoriseraient ses concurrents. Il peut s'agir d'un programme informatique particulier (par exemple un programme de modélisation) ou de détails de ce programme. Si les informations commerciales confidentielles peuvent être aisémentséparées des informations qui font l'objet d'une demande d'accès, l'organisation doit procéder à la séparation des données confidentielles et répondre à la demande. Les organisations peuvent refuser ou limiter l'accès si elles risquent de voir divulguées leur informations commerciales confidentielles telles qu'elles sont définies ci-dessus — notamment les inférences ou les classifications commerciales établies par l'organisation — ou des informations commerciales confidentielles appartenant à d'autres organisations, si ces informations sont soumises à une obligation contractuelle de confidentialité dans les cas où une telle obligation serait normalement mise en œuvre ou imposée.

Q 3: *Lorsqu'elle fournit un accès, l'organisation peut-elle communiquer aux personnes concernées des informations à caractère personnel tirées de ses bases de données ou doit-elle permettre l'accès à cette base de données?*

R 3: L'accès peut être fourni sous la forme d'un transfert d'informations à la personne concernée et n'implique pas obligatoirement que cette dernière consulte la base de données de l'organisation.

Q 4: *L'organisation doit-elle restructurer ses bases de données afin de permettre l'accès?*

R 4: L'accès ne doit être fourni que dans la mesure où l'organisation stocke les informations. Le principe d'accès en soi ne crée aucune obligation de conservation, de gestion, de réorganisation ou de restructuration des fichiers d'informations personnelles.

Q 5: *Ces réponses établissent clairement que l'accès peut parfois être refusé. Dans quelles autres circonstances l'organisation peut-elle refuser à une personne qui le souhaite d'accéder aux informations personnelles qu'elle détient à son sujet?*

R 5: Ces circonstances sont limitées et les motifs justifiant le refus de l'accès doivent être spécifiques. L'organisation peut refuser l'accès à certaines informations pour autant que leur diffusion risque de porter atteinte à d'importants intérêts publics, tels que la sécurité nationale, la défense ou la sécurité publique. L'accès peut également être refusé lorsque les informations personnelles sont traitées *uniquement* à des fins statistiques ou de recherche. D'autres motifs justifient le refus ou la limitation de l'accès:

a) une entrave à l'exécution ou à l'application de la loi, notamment à la prévention de la criminalité, à la détection des infractions et délits et aux enquêtes y afférentes ou encore au droit à un procès équitable;

b) une entrave aux actions civiles en justice, notamment à la prévention et à la détection d'actions en justice et aux enquêtes y afférentes ou encore au droit à un procès équitable;

c) la diffusion d'informations faisant référence à une ou plusieurs autres personnes si ces références ne peuvent être traitées;

▼B

d) le non-respect d'une obligation ou d'un privilège légal ou professionnel;

e) le non-respect de la confidentialité indispensable dans le cadre de négociations futures ou en cours, telles que celles concernant l'acquisition de sociétés cotées en Bourse;

f) une entrave aux enquêtes sur la sécurité des employés et aux procédures d'arbitrage;

g) le fait de compromettre la confidentialité qui peut s'avérer nécessaire pendant de courtes périodes lors de l'organisation des remplacements et des restructurations;

h) le fait de porter atteinte à la confidentialité qui peut s'avérer nécessaire au contrôle, à l'inspection ou aux fonctions réglementaires en rapport avec une gestion économique ou financière saine;

i) d'autres circonstances où l'accès entraînerait une charge ou des coûts disproportionnés et qu'il y aurait violation des droits ou des intérêts légitimes de tiers.

Il incombe à l'organisation qui invoque l'exception d'en prouver le bien-fondé (ce qui est généralement le cas). Comme cela a déjà été précisé, les raisons du refus ou de la limitation de l'accès doivent être données aux personnes qui ont introduit la demande et il convient de leur communiquer les coordonnées d'une personne à contacter pour plus d'informations.

Q 6: *Une organisation peut-elle rendre l'accès payant pour couvrir ses frais?*

R 6: Oui. Les lignes directrices de l'OCDE reconnaissent que les organisations peuvent demander le paiement d'une redevance, pour autant qu'elle ne soit pas excessive. Les organisations peuvent donc fixer une participation équitable aux frais d'accès. Le fait de rendre l'accès payant peut contribuer à lutter contre les demandes répétitives et vexatoires.

Le organisations spécialisées dans la vente d'informations accessibles au public peuvent donc répondre à des demandes d'accès contre le paiement d'une participation correspondant au montant habituellement demandé par l'organisation. Chacun peut, par ailleurs, obtenir les informations qui le concernent en s'adressant directement à la première organisation qui a compilé les données.

L'accès ne peut pas être refusé pour des raisons de coût si la personne concernée propose de prendre en charge les frais occasionnés.

Q 7: *Une organisation est-elle obligée de permettre l'accès aux informations à caractère personnel tirées des registres publics?*

R 7: Précisons, tout d'abord, que les registres publics sont des registres conservés par les services des autorités gouvernementales ou d'autres administrations publiques à quelque niveau que ce soit qui peuvent être consultés par tous. Les principes d'accès ne doivent pas être appliqués à ces informations si ces dernières ne sont pas associées à d'autres données à caractère personnel, sauf si quelques informations non publiques sont utilisées pour indexer ou organiser les registres publics. Toutefois, les conditions de consultation fixées par les instances compétentes doivent être respectées. Lorsque des informations tirées de ces registres sont associées à d'autres données non publiques (exception faite du cas précisé ci-dessus), l'organisation est tenue d'en permettre l'accès, pour autant que ces informations ne font pas l'objet d'autres dérogations.

Q 8: *Le principe de l'accès doit-il être appliqué aux informations personnelles accessibles au public?*

R 8: Tout comme dans le cas des informations tirées des registres publics (voir Q 7), il n'est pas nécessaire d'accorder l'accès aux informations qui sont déjà à la disposition du public, pour autant que ces informations ne sont pas associées à d'autres données non publiques.

Q 9: *Comment l'organisation peut-elle lutter contre les demandes d'accès répétitives ou vexatoires?*

R 9: L'organisation n'est pas tenue de répondre à de telles demandes d'accès. C'est pour cette raison qu'elle peut demander le paiement d'une participation équitable aux frais et fixer une limite acceptable au nombre de demandes d'accès déposées au cours d'une période donnée. Lorsqu'elle fixe ces limites, l'organisation doit tenir compte de facteurs tels que la fréquence de mise à jour des informations, le but de l'utilisation des données et la nature des informations.

Q 10: *Comment l'organisation peut-elle se protéger contre les demandes d'accès frauduleuses?*

▼B

R 10: L'organisation n'est pas tenue de fournir l'accès si elle ne reçoit pas les informations nécessaires à l'identification du demandeur.

Q 11: *La réponse à la demande d'accès doit-elle être fournie dans un délai précis?*

R 11: Oui, les organisations doivent répondre dans un délai raisonnable. Cette condition peut être remplie de différentes manières, comme le précise l'exposé des motifs des lignes directrices de l'OCDE sur la protection de la vie privée (1980). Ainsi, un responsable de données qui fournit régulièrement des informations aux personnes concernées peut être exempté de l'obligation de répondre immédiatement aux demandes individuelles.

FAQ 9 — Ressources humaines

Q 1: *Le transfert de l'Union européenne vers les États-Unis d'informations personnelles rassemblées dans le cadre d'une relation de travail est-il couvert par la «sphère de sécurité»?*

R 1: Oui, si une société située dans l'Union européenne transfère des informations personnelles relatives à ses salariés (actuels ou anciens) et rassemblées dans le cadre d'une relation de travail à une société mère, affiliée ou non affiliée qui fournit des services aux États-Unis et qui adhère aux principes de la «sphère de sécurité», ce transfert bénéficiede la «sphère de sécurité». Dans ce cas, la collecte d'informations ainsi que son traitement avant le transfert sont soumis aux lois nationales du pays de l'Union européenne où la collecte est réalisée et toutes les conditions ou les restrictions fixées en la matière par celles-ci doivent être respectées.

Les principes de la «sphère de sécurité» ne sont pertinents qu'en cas de transfert ou d'accès à des dossiers individuels identifiés. La déclaration statistique fondée sur les données globales en matière d'emploi et/ou l'utilisation de données rendues anonymes ou de pseudonymes ne présentent pas de risques pour la vie privée.

Q 2: *Comment les principes de notification et de choix s'appliquent-ils à ces données?*

R 2: Une organisation américaine qui a reçu de l'Union européenne des informations sur les salariés dans le cadre de la «sphère de sécurité» peut les communiquer à des tiers et/ou les utiliser à d'autres fins uniquement si les principes qui régissent la notification et le choix sont respectés. Par exemple, si une organisation américaine veut utiliser les informations personnelles rassemblées dans le cadre d'une relation de travail dans un but qui n'est pas lié à cette relation de travail — par exemple l'envoi de messages de *marketing* —, elle doit laisser le choix aux personnes concernées au préalable, à moins que celles-ci n'aient déjà donné leur autorisation pour que les informations soient utilisées à de telles fins. En outre, l'employeur ne peut utiliser les choix exprimés pour entraver la carrière professionnelle de ses salariés ou prendre des sanctions à leur égard.

Il convient de signaler que certaines conditions applicables de manière générale au transfert à partir de quelques États membres peuvent exclure d'autres utilisations de ces informations, même après leur transfert en dehors du territoire de l'Union européenne, et que ces conditions doivent être respectées.

Par ailleurs, les employeurs doivent s'efforcer de tenir compte des préférences du salarié en ce qui concerne la protection de sa vie privée. Il peut s'agir, par exemple, de restreindre l'accès aux données, d'en rendre certaines anonymes ou de leur attribuer des codes ou pseudonymes lorsque l'objectif de gestion poursuivi ne requiert pas l'utilisation des vrais noms.

Dans la mesure nécessaire et pour aussi longtemps que nécessaire, pour éviter de léser les intérêts légitimes de l'organisation dans le cadre de promotions, d'engagements ou d'autres décisions similaires relatives à l'emploi, une organisation n'est pas tenue de respecter le principe de la notification et du choix.

Q 3: *Comment le principe de l'accès s'applique-t-il?*

R 3: Les FAQ concernant le principe d'accès fournissent des indications sur les raisons qui peuvent justifier le refus ou la restriction de l'accès demandé dans le contexte des ressources humaines. Dans l'Union européenne, les employeurs doivent naturellement respecter les réglementations locales et veiller à ce que les salariés de l'Union européenne aient accès à ces informations, conformément à la loi de leur pays d'origine, quel que soit le lieu de traitement et de conservation des données. Dans le contexte de la «sphère de sécurité», une organisation traitant de telles données aux

▼B

États-Unis doit coopérer en fournissant cet accès, soit directement, soit par le biais de l'employeur de l'Union européenne.

Q 4: *Comment la mise en œuvre sera-t-elle assurée à l'égard des données des salariés dans le cadre de la «sphère de sécurité»?*

R 4: Dans la mesure où les informations sont utilisées uniquement dans le cadre d'une relation de travail, la responsabilité principale des données vis-à-vis du salarié incombe toujours à la société située dans l'Union européenne. C'est la raison pour laquelle, si un salarié européen se plaint du non-respect de son droit à la protection des données et n'est pas satisfait des résultats des procédures internes d'évaluation, de réclamation et d'appel (ou de toute procédure d'arbitrage applicable en vertu d'un contrat conclu avec un syndicat), il convient de l'orienter vers les autorités nationales responsables des questions du travail ou de la protection des données dans la juridiction où il travaille. Cela comprend également les cas où le mauvais usage allégué de l'information personnelle a eu lieu aux États-Unis et relève de la responsabilité de l'organisation américaine qui a reçu l'information de l'employeur, et non de l'employeur, et entraîne donc une violation alléguée des principes de la «sphère de sécurité», plutôt que des dispositions législatives nationales transposant la directive. C'est le moyen le plus efficace de résoudre les chevauchements qui existent souvent entre les droits et obligations définis par la législation du travail et les conventions collectives locales ainsi que par la loi relative à la protection des données.

Une organisation américaine adhérant aux principes de la «sphère de sécurité» qui utilise des données de l'Union européenne concernant les ressources humaines transférées à partir de l'Union européenne dans le cadre d'une relation de travail et qui souhaite que ces transferts soient couverts par la «sphère de sécurité» doit s'engager à cet effet à coopérer aux enquêtes des autorités compétentes de l'Union européenne et à respecter l'avis de celles-ci.Les autorités chargées de la protection des données qui sont convenues de coopérer dans ce sens en informeront la Commission européenne et le ministère du commerce. Si une organisation américaine qui adhère aux principes de la «sphère de sécurité» souhaite transférer des données concernant les ressources humaines à partir d'un État membre où l'autorité chargée de la protection des données n'a pas convenu d'un tel accord, les dispositions prévues par la FAQ 5 seront applicables.

FAQ 10 — Contrats au titre de l'article 17

Q: *Le transfert de l'Union européenne vers les États-Unis de données uniquement pour des besoins de sous-traitement nécessite-t-il un contrat indépendamment de la participation du responsable du sous-traitement à la «sphère de sécurité»?*

R: Oui. Un contrat est toujours exigé de la part des responsables de traitement européens pour un transfert en vue d'un sous-traitement pur, que cette opération soit effectuée à l'intérieur ou à l'extérieur de l'Union européenne. Le but du contrat est de protéger les intérêts du responsable de traitement, c'est-à-dire la personne ou l'organisme qui détermine les finalités et les moyens du traitement et porte l'entière responsabilité des données vis-à-vis des personnes concernées. Le contrat spécifie donc le traitement à effectuer et toutes les mesures nécessaires pour garantir la sécurité des données.

Par conséquent, une organisation américaine couverte par la «sphère de sécurité» et recevant des informations personnelles de l'Union européenne pour sous-traitement n'a pas à appliquer les principes à ces informations puisque le responsable de traitement européen reste responsable vis-à-vis des personnes, conformément aux dispositions communautaires en la matière (qui peuvent être plus rigoureuses que les principes de «sphère de sécurité» équivalents).

Étant donné que les participants à la «sphère de sécurité» assurent une protection adéquate, les contrats de sous-traitement pur conclus avec ces derniers ne nécessitent pas d'autorisation préalable (ou alors cette autorisation est octroyée automatiquement par les États membres), contrairement aux contrats dont les bénéficiaires ne participent pas à la «sphère de sécurité» ou qui n'assurent pas de protection adéquate.

FAQ 11 — Résolution des litiges et application des décisions

Q: *Comment les exigences en matière de résolution des litiges formulées dans le principe d'application doivent-elles être mises en œuvre et comment le*

▼B

non-respect persistant des principes de la part d'une organisation sera-t-il traité?

R: Le principe d'application définit les exigences sur lesquelles repose la mise en œuvre de la «sphère de sécurité». La FAQ sur la vérification (FAQ 7) explique la manière de satisfaire les exigences énoncées au point b) du principe. La présente FAQ 11 traite des points a) et c), qui nécessitent tous deux des instances de recours indépendantes. Ces instances peuvent prendre différentes formes, mais doivent répondre aux exigences du principe d'application. Les organisations participant à la «sphère de sécurité» peuvent les satisfaire: 1) en participant à des programmes du secteur privé en matière de protection de la vie privée intégrant dans leurs règles les principes de la «sphère de sécurité» et comportant des mécanismes de mise en œuvre efficaces, de même nature que ceux qui sont décrits dans le principe d'application; 2) en se conformant aux instructions des organes légaux ou statutaires de surveillance qui assurent le traitement des plaintes de particuliers et la résolution des litiges; 3) en s'engageant à coopérer avec les autorités chargées de la protection des données au sein de la Communauté européenne ou avec leurs représentants autorisés. La présente liste a valeur indicative et n'est pas restrictive. Le secteur privé peut concevoir d'autres mécanismes de mise en application, pour autant que ceux-ci répondent aux exigences du principe d'application et des FAQ. Il convient de remarquer que les exigences du principe d'application s'ajoutent à l'exigence énoncée au paragraphe 3 de l'introduction aux principes, selon laquelle les initiatives d'autoréglementation doivent être exécutoires conformément à la section 5 du Federal Trade Commission Act ou à une loi similaire.

Instances de recours

Les consommateurs devraient être encouragés à soumettre toute plainte éventuelle à l'organisation concernée avant de faire appel à des instances de recours indépendantes. L'indépendance d'une instance de recours est à apprécier selon des critères objectifs, tels que la transparence de sa composition et de son financement ou un bilan positif dans son domaine d'activité. Comme le prévoit le principe d'application, le recours dont disposent les particuliers doit être facilement accessible et abordable économiquement. Les organismes d'instruction des litiges devraient étudier toutes les plaintes déposées par des particuliers, à moins qu'elles ne soient manifestement non fondées ou abusives. Cette condition n'empêche pas l'établissement, par l'instance de recours, de critères d'éligibilité, mais ceux-cidevraient être transparents et justifiés (ils pourraient viser, par exemple, à exclure les plaintes qui ne rentrent pas dans le champ d'application du programme ou qui relèvent des compétences d'une autre instance) et ne devraient pas avoir pour effet de compromettre l'engagement à examiner les plaintes légitimes. Les instances de recours devraient, en outre, fournir aux particuliers des informations complètes et facilement accessibles sur le fonctionnnement de la procédure lors du dépôt de la plainte. Ces informations devraient inclure une description des pratiques suivies en matière de protection de la vie privée, conformément aux principes de la sphère de sécurité ([1]). Les instances devraient, en outre, coopérer en vue de mettre au point des outils, tels que des formulaires standards de plainte, destinés à faciliter le fonctionnement de la procédure de résolution des litiges.

Recours et sanctions

Tout recours auprès de l'organisme d'instruction des litiges devrait aboutir à l'annulation ou à la correction, dans la mesure du possible, des effets du non-respect des principes par l'organisation, au respect des principes lors des traitements futurs par cette même organisation et, le cas échéant, à l'arrêt du traitement des données personnelles de la personne qui a déposé la plainte. Les sanctions doivent être suffisamment sévères pour garantir le respect des principes de la part de l'organisation. Une série de sanctions

([1]) Les instances de résolution des litiges ne sont pas tenues de se conformer au principe d'application. Elles peuvent également déroger aux principes si elles sont confrontées à des obligations contradictoires ou reçoivent des autorisations explicites lors de la réalisation des tâches spécifiques relevant de leurs compétences.

▼B

ayant des degrés de sévérité différents permettra aux instances de résolution des litiges de répondre de manière adéquate à des niveaux différents de non-respect. Les sanctions doivent inclure à la fois la publication des violations et l'obligation d'effacer les données dans certaines circonstances [1]. D'autres sanctions pourraient être la suspension ou le retrait de l'agrément, l'indemnisation des pertes subies par les particuliers en raison du non-respect et des injonctions. Les organismes de résolution des litiges et d'autoréglementation du secteur privé doivent signaler aux tribunaux ou aux pouvoirs publics compétents, selon le cas, les organisations adhérant aux principes de la «sphère de sécurité» qui ne respectent pas leurs décisions et en informer le ministère du commerce (ou la personne désignée par celui-ci).

Action de la FTC

La FTC 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 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. Si la FTC conclut qu'il y a lieu de croire que la section 5 a été violée, elle peut résoudre l'affaire en obtenant une injonction administrative de cessation interdisant les pratiques contestées ou en déposant une plainte auprès d'une cour de district fédérale qui, si la plainte aboutit, peut rendre un arrêt dans le même sens. La FTC peut requérir des sanctions civiles en cas de violation d'une injonction administrative de cessation et poursuivre le contrevenant pour outrage au tribunal de nature civile ou criminelle s'il viole l'arrêt d'une cour fédérale. La FTC informe le ministère du commerce de toute action de ce type qu'elle entreprend. Le ministère du commerce encourage les autres organismes publics à lui communiquer l'issue de toutes les affaires analogues ou d'autres décisions déterminant l'adhésion aux principes.

Non-respect persistant

Si une organisation ne respecte par les principes de manière persistante, elle n'est plus en droit de bénéficier des avantages de la «sphère de sécurité». Il y a non-respect persistant lorsqu'une organisation qui a déclaré son adhésion aux principes au ministère du commerce (ou à la personne désignée par celui-ci) refuse de se conformer à une décision définitive prise par un organisme d'autoréglementation ou un organisme public, ou qu'un tel organisme constate qu'elle viole fréquemment les principes, au point que sa déclaration d'adhésion n'est plus crédible. L'organisation doit alors en informer sans retard le ministère du commerce (ou la personne désignée par celui-ci). Dans le cas contraire, elle est passible de sanctions en vertu du False Statements Act.

Le ministère du commerce (ou la personne désignée par celui-ci) 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, qu'elle provienne de l'organisation elle-même, d'un organisme d'autoréglementation ou d'un organisme public, 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 (ou la personne désignée par celui-ci) précisera donc quelles organisations bénéficient des avantages de la «sphère de sécurité» et quelles organisations n'en bénéficient plus.

Toute organisation demandant à être soumise à l'autorité d'un organisme d'autoréglementation afin de pouvoir bénéficier à nouveau des avantages de la «sphère de sécurité» devra fournir à cet organisme des informations exhaustives sur son adhésion antérieure aux principes.

FAQ 12 — Choix (le droit d'opposition) — Quand peut-il être exercé?

Q: *Le principe du choix permet-il à la personne concernée d'opérer un choix seulement au début des relations ou à tout moment?*

[1] Les circonstances dans lesquelles ces sanctions doivent être appliquées sont laissées à l'appréciation des organismes de résolution des litiges. Lorsque l'on décide s'il convient d'exiger l'effacement des données, il faut notamment prendre en compte le caractère sensible des informations concernées et déterminer si elles ont été collectées, employées ou dévoilées en violation manifeste des principes.

▼B

R: D'une manière générale, le principe du choix a pour but de s'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). L'organisation peut également requérir un certain nombre d'informations pour confirmer l'identité de la personne qui fait part de son opposition. Aux États-Unis,ce droit peut être exercé par le biais d'un programme central de refus, tel que le «mail preference service» de la Direct Marketing Association. Les organisations participant au «mail preference service» de la Direct Marketing Association devraient promouvoir la disponibilité de celui-ci auprès des consommateurs ne souhaitant pas recevoir d'informations commerciales. En tout état de cause, le recours à cette option doit être facile et peu coûteux.

De même, une organisation peut utiliser des informations à certaines fins de *marketing* direct lorsque les conditions ne permettent pas de laisser le choix avant l'utilisation des données, à condition qu'elle donne ensuite rapidement (et à tout moment sur demande) aux personnes concernées la possibilité de refuser, sans aucun frais, toute autre communication de *marketing* direct et qu'elle se conforme aux souhaits de ces dernières.

FAQ 13 — Information sur les voyages

Q: *Quand peut-on communiquer aux organisations situées en dehors de l'Union européenne les informations concernant les passagers des transports aériens (fournies notamment lors des réservations), telles que celles concernant les clients réguliers ou les réservations d'hôtel ainsi que les demandes spéciales — par exemple la composition des repas conformément à certains principes religieux ou une assistance physique?*

R: Ces informations peuvent être transférées dans différentes circonstances. Conformément à l'article 26 de la directive, les données à caractère personnel peuvent être transférées vers un pays tiers n'assurant pas un niveau de protection adéquat au sens de l'article 25, paragraphe 2, à condition 1) que le transfert soit nécessaire à la prestation des services demandés par le client ou à l'exécution d'un contrat, tel qu'un contrat «de fidélité», ou 2) que le passager ait indubitablement donné son consentement. Les organisations américaines adhérant aux principes de la «sphère de sécurité» assurent une protection adéquate des données à caractère personnel et peuvent donc recevoir ces données de l'Union européenne sans satisfaire à ces conditions ni aux autres conditions spécifiées par l'article 26 de la directive. Étant donné que les principes de la «sphère de sécurité» comportent des règles spécifiques concernant les informations sensibles, ce type d'information (pouvant concerner, par exemple, la nécessité, pour un client, de bénéficier d'une assistance physique) peut figurer parmi les données transférées aux organisations adhérant aux principes de la «sphère de sécurité». L'organisation transférant l'information doit cependant appliquer dans chaque cas la législation nationale de l'État membre de l'Union européenne où elle opère, laquelle législation peut *entre autres* imposer des conditions spéciales au traitement des données sensibles.

FAQ 14 — Produits pharmaceutiques et médicaux

Q 1: *Si les données personnelles sont recueillies au sein de l'Union européenne et transférées aux États-Unis pour la recherche pharmaceutique et/ou à d'autres fins, applique-t-on les législations des États membres ou les principes relatifs à la «sphère de sécurité»?*

R 1: La législation des États membres s'applique à la collecte des données personnelles et à tout traitement intervenant avant le transfert aux États-Unis. Les principes relatifs à la «sphère de sécurité» s'appliquent aux données une fois qu'elles ont été transférées aux États-Unis. Les données utilisées pour la recherche pharmaceutique et à d'autres fins devraient être rendues anonymes le cas échéant.

Q 2: *Les données personnelles élaborées dans le cadre d'études médicales ou pharmaceutiques jouent souvent un rôle précieux dans la recherche scientifique. Lorsque les données personnelles recueillies pour une étude sont transférées à une organisation des États-Unis dans la «sphère de sécurité», cette organisation peut-elle utiliser les données pour une nouvelle activité de recherche scientifique?*

▼B

R 2: Oui, s'il a été prévu au départ une notification et un choix approprié. Cette notification doit fournir des informations sur toute utilisation spécifique future des données, telles que le suivi périodique, les études associées ou la commercialisation. Toutes les utilisations futures des données ne peuvent être spécifiées, puisqu'un nouvel examen des données originales, des découvertes et progrès médicaux nouveaux et des évolutions en matière de santé publique et de réglementation peuvent engendrer de nouvelles utilisations de la recherche. La notification devrait donc inclure, le cas échéant, une indication que les données personnelles peuvent être utilisées pour des activités de recherche médicale et pharmaceutique futures non planifiées à l'avance. Si cette utilisation n'est pas cohérente avec les objectifs de recherche généraux pour lesquels les données ont été originalement recueillies ou auxquels la personne concernée a consenti par la suite, il convient d'obtenir un nouveau consentement.

Q 3: *Que deviennent les données individuelles si un participant décide volontairement ou à la demande du commanditaire de se retirer de l'essai clinique?*

R 3: Les participants peuvent à tout moment décider de se retirer d'un essai clinique ou être priés de le faire. Toutes les données recueillies avant le retrait peuvent encore être traitées avec les autres données recueillies dans le cadre de l'essai clinique, à condition que cela ait été précisé au participant dans la notification au moment où il a donné son accord.

Q 4: *Les sociétés d'appareils pharmaceutiques et médicaux ont le droit de fournir des données personnelles extraites des essais cliniques réalisés dans l'Union européenne aux autorités des États-Unis à des fins de réglementation et de contrôle. Ce type de transfert est-il permis à d'autres parties telles qu'entreprises et autres chercheurs?*

R 4: Oui, en conformité avec les principes de notification et de choix.

Q 5: *Pour garantir l'objectivité de nombreux essais cliniques, l'accès aux informations relatives au traitement reçu par les participants est interdit à ceux-ci et, fréquemment, aussi aux chercheurs. Cela mettrait en question la validité de l'étude et des résultats de la recherche. Les participants à ces essais cliniques (qualifiés d'études «masquées» auront-ils accès aux données relatives à leur traitement pendant l'essai?*

R 5: Non, l'accès ne doit pas être accordé au participant si cette restriction lui a été expliquée lorsqu'il a commencé l'essai et si la révélation de cette information était susceptible de nuire à l'intégrité de l'effort de recherche. L'accord à la participation à l'essai dans ces conditions implique de renoncer au droit d'accès. Après l'achèvement de l'essai et l'analyse des résultats, les participants devraient avoir accès à leurs données s'ils le demandent. Ils devraient le demander, en premier lieu, au médecin ou autre prestataire de soins de santé qui les a traités pendant l'essai clinique ou, en second lieu, auprès de la société commanditaire.

Q 6: *Les sociétés d'appareils pharmaceutiques ou médicaux doivent-elles appliquer à leurs activités de contrôle de la sécurité et de l'efficacité du produit les principes de la «sphère de sécurité» en ce qui concerne la notification, le choix, le transfert et l'accès à celles-ci, y compris le compte rendu d'incidents et le suivi des malades ou sujets impliquant l'utilisation de certains médicaments ou appareils médicaux (par exemple, un stimulateur cardiaque)?*

R 6: Non, dans la mesure où le respect de ces principes entre en conflit avec les exigences réglementaires. Cela est vrai pour ce qui concerne, par exemple, les rapports effectués tant par les prestataires de soins de santé aux sociétés d'appareils pharmaceutiques et médicaux que par les sociétés d'appareils pharmaceutiques et médicaux à des agences gouvernementales telles que la Food and Drug Administration (organisme de surveillance des aliments et des médicaments).

Q 7: *Les données de la recherche sont habituellement codées à leur source uniquement par le chercheur principal, pour ne pas révéler l'identité des intéressés. Les sociétés pharmaceutiques qui commanditent ce type de recherche ne reçoivent pas la clé de ce code. Le code de la clé unique est détenu par le seul chercheur, pour qu'il puisse identifier la personne concernée dans des circonstances spéciales (par exemple, si un suivi médical est requis). Le transfert de l'Union européenne aux États-Unis de données personnelles ainsi codées représente-t-il un transfert de données soumis aux principes de la «sphère de sécurité»?*

R 7: Non. Cela ne représenterait pas un transfert de données personnelles soumis à ces principes.

▼B

FAQ 15 — Informations des registres publics et informations accessibles au public

Q: *Faut-il appliquer les principes de notification, de choix et de transfert ultérieur aux informations des registres publics ou aux informations accessibles au public?*

R: Les principes de notification, de choix ou de transfert ultérieur ne doivent pas être appliqués aux informations des registres publics si ces dernières ne sont pas combinées à des informations non publiques et si les conditions de consultation établies par la juridiction compétente sont respectées.

Les informations accessibles au public ne requièrent pas davantage l'application des principes de notification, de choix ou de transfert ultérieur, à moins que l'auteur européen du transfert ne précise qu'elles font l'objet de restrictions qui exigent l'application de ces principes lors de leur utilisation par l'organisation. L'organisation ne sera pas tenue responsable de l'utilisation faite de ces informations par ceux qui les tirent de publications.

S'il s'avère qu'une organisation a volontairement publié des données à caractère personnel en violation des principes de manière qu'elle-même ou des tiers puissent bénéficier de ces exceptions, elle sera exclue de la «sphère de sécurité»

▼B

ANNEXE III

Étude relative à la mise en œuvre des principes de la «sphère de sécurité»

Pouvoirs de l'État fédéral et des États fédérés en matière de pratiques déloyales et frauduleuses et protection de la vie privée

Le présent aide-mémoire donne un aperçu général des pouvoirs conférés à la Federal Trade Commission (FTC) par la section 5 du Federal Trade Commission Act (15 USC, §§ 41-58, sous sa forme modifiée) pour prendre des mesures contre les personnes dont les pratiques en matière de protection des informations à caractère personnel ne sont pas conformes à leurs déclarations et/ou engagements. Il aborde également les dérogations à ces pouvoirs et les possibilités d'intervention dont disposent d'autres organismes publics, au niveau tant fédéral que fédéré, lorsque la FTC n'est pas compétente (1).

Pouvoirs de la FTC en matière de pratiques déloyales ou frauduleuses

La section 5 du Federal Trade Commission Act déclare illégales les «manœuvres et pratiques déloyales ou frauduleuses dans le domaine du commerce» [15 USC, § 45 a) 1)]. Elle confère à la FTC les pleins pouvoirs pour empêcher de tels agissements [15 USC, § 45 a) 2)]. Par voie de conséquence, la FTC peut, après avoir procédé à une audition officielle, émettre une «ordonnance de cessation» en vue de mettre fin au comportement infractionnel [15 USC, § 45 b)]. Si l'intérêt public l'exige, la FTC peut également demander à un tribunal de première instance des États-Unis (*US district court*) la délivrance d'une ordonnance de ne pas faire temporaire ou d'une injonction temporaire ou permanente [15 USC, § 53 b)]. Lorsque les manœuvres et pratiques déloyales ou frauduleuses ont un caractère systématique ou que la FTC a déjà rendu des ordonnances de cessation y afférentes, cette dernière peut édicter des prescriptions administratives relatives aux manœuvres ou pratiques concernées [15 USC, § 57 a)].

Quiconque ne se conforme pas à une ordonnance de la FTC peut être condamné, au civil, à une astreinte pouvant aller jusqu'à 11 000 dollars des États-Unis, chaque jour d'une violation persistante constituant une violation distincte (2) [15 USC, § 45 1)]. De même, quiconque viole délibérément une prescription de la FTC est passible d'une astreinte de 11 000 dollars pour chaque violation [15 USC, § 45 m)]. Les actions visant à assurer l'application de la législation peuvent être intentées soit par le ministère de la justice, soit, si celui-si s'abstient de faire usage de ses prérogatives, par la FTC (15 USC, § 56).

Pouvoirs de la FTC et protection de la vie privée

Dans 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'informations auprès des consommateurs et sur la façon dont ces informations seront utilisées constitue une pratique frauduleuse (3). En 1998, la FTC a, par exemple, déposé une plainte contre la société GeoCities, qui, contrairement à ses déclarations et sans autorisation préalable, avait divulgué à des tiers, à des fins publicitaires, des

(1) La présente étude nesse pas en revue l'ensemble des dispositions fédérales traitant de la protection de la vie privée dans des contextes particuliers ni les dispositions des différents États fédérés et la *common law* susceptibles de s'appliquer. Parmi les lois qui, au niveau fédéral, réglementent la collecte et l'utilisation, à des fins commerciales, des informations à caractère personnel figurent les textes suivants: Cable Communications Policy Act (47 USC, § 551), Dirver's Privacy Protection Act (18 USC, § 2721), Electronic Communications Privacy Act (18 USC, § 2701 et suivantes), Eletronic Funds Transfer Act [15 USC, §§ 1693, 1693 m)], Fair Credit Reporting Act (15 USC, § 1681 et suivantes), Right to Financial Privacy Act (12 USC, § 3401 et suivantes), Telephone Consumer Protection Act (47 USC, § 227), Video Privacy Protection Act (18 USC, § 2710). De nombreux États fédérés ont une législation analogue dans ces domaines. Voir, par exemple: Mass. Gen. Laws, chapitre 167B, § 16 (interdisant aux établissements financiers de divulguer des informations financières sur leurs clients à des tiers sans le consentement des clients ou sans une décision de justice correspondante); NY Pub. Health Law, § 17 (limitant l'utilisation et la divulgation des données sur la santé physique ou mentale et accordant aux patients un droit d'accès à ces données).

(2) Dans le cadre d'une telle action en justice, le tribunal de première instance des États-Unis (United States district court) peut également ordonner des mesures de redressement par voie d'injonction et en équité jugées propres à faire exécuter l'ordonnance de la FTC [15 USC, § 45 1)].

(3) Une «pratique frauduleuse» se définit comme une déclaration, une omission ou une pratique susceptibles d'induire en erreur, de façon significative, le consommateur normalement avisé.

▼B

informations collectées sur son site web [1]. Les services de la FTC ont également indiqué que la collecte d'informations personnelles auprès d'enfants ainsi que la vente et la divulgation de ces informations sans le consentement des parents étaient susceptibles de constituer une pratique déloyale [2].

Dans une lettre adressée à M. John Mogg, directeur général à la Commission européenne, M. Pitofsky, président de la FTC, a fait observer que les pouvoirs de la FTC en matière de protection de la vie privée étaient limités en l'absence de fausse déclaration (ou de quelque déclaration que ce soit) sur l'utilisation ultérieure des informations [voir lettre de M. Pitofsky, président de la FTC, à M. John Mogg (23 septembre 1998)]. Toutefois, les entreprises souhaitant bénéficier de la «sphère de sécurité» envisagée devront certifier que les informations collectées par leurs soins seront protégées conformément aux lignes directrices prescrites. De ce fait, toute entreprise qui certifiera qu'elle garantira la confidentialité des informations et qui ne respectera pas cet engagement se rendra coupable de fausse déclaration et se livrera à une «pratique frauduleuse» au sens de la section 5.

La compétence de la FTC couvre les manœuvres et pratiques déloyales ou frauduleuses «dans le domaine du commerce» et ne s'étend donc pas à la collecte et à l'utilisation d'informations personnelles à des fins non commerciales (collecte de fonds au profit d'œuvres de bienfaisance, par exemple) (lettre de M. Pitofsky, p. 3). En revanche, l'utilisation d'informations personnelles dans tout type de transaction commerciale relève de la compétence de la FTC. Lorsqu'un employeur vend, par exemple, des informations à caractère personnel relatives à ses salariés à une société de *marketing* direct, la transaction tombe dans le champ d'application de la section 5.

Dérogations prévues par la section 5

La section 5 prévoit des dérogations à la compétence de la FTC en matière de manœuvres et pratiques déloyales ou frauduleuses pour les secteurs d'activité suivants:

— les établissements financiers, y compris les banques, les entreprises financières d'épargne et de prêt et les coopératives de crédit,

— les sociétés de télécommunications et les entreprises publiques de transport inter-États,

— les transporteurs aériens,

— les conditionneurs et les exploitants de parcs à bestiaux.

Voir 15 USC, § 45 a) 2). Ces différentes dérogations et les organismes de réglementation se substituant à la FTC sont examinés ci-dessous.

(1) Voir www.ftc.gov/opa/1998/9808/geocitie.htm

(2) Voir lettre de la FTC au Center for Media Education, (www.ftc.gov/os/1997/9707/cenmed.htm). Par ailleurs, le Children's Online Privacy Protection Act de 1998 confère à la FTC des pouvoirs juridiques spécifiques pour réglementer la collecte d'informations personnelles auprès d'enfants par des exploitants de sites web et de services en ligne (15 USC, §§ 6501-6506). La loi fait notamment obligation à de tels exploitants de prévoir un avis d'information et d'obtenir le consentement vérifiable des parents avant de collecter, d'utiliser ou de divulguer des informations personnelles données par des enfants [15 USC, § 6502 b)]. Elle accorde également aux parents le droit d'accéder aux informations collectées et de refuser l'autorisation nécessaire à la poursuite de leur utilisation (*idem*).

▼B

Établissements financiers (1)

La première dérogation vise «les banques, les établissements d'épargne et de prêt au sens de la section 18 f) 3) [15 USC, § 57 a) f) 3)] » ainsi que les «coopératives fédérales de crédit au sens de la section 18 f) 4) [15 USC, § 57 a) f) 4)]» (2). Au lieu de relever de la FTC, ces établissements financiers sont soumis à des dispositions arrêtées respectivement par le Federal Reserve Board, l'Office of Thrift Supervision (3) et le National Credit Union Administration Board [15 USC, § 58 a) f)]. Ces organes de réglementation sont tenus d'adopter les dispositions nécessaires pour emplêcher les établissements financiers précités de se livrer à des pratiques déloyales ou frauduleuses (4) et doivent créer des services distincts chargés de traiter les plaintes des consommateurs [15 USC, § 57 a) f) 1)]. Enfin, les compétences d'exécution découlent de la section 8 du Federal Deposit Insurance Act (12 USC, § 1818) pour les banques et les établissements d'épargne et de prêt et des sections 120 et 206 du Federal Credit Union Act pour les coopératives fédérales de crédit [15 USC, §§ 57 a) f) 2)-4)].

Même si les compagnies d'assurances ne sont pas expressément citées dans la liste des dérogations figurant à la section 5, la loi McCarran-Ferguson (15 USC, § 1011 et suivantes) dispose, d'une manière générale, que la réglementation desactivités d'assurance incombe aux différents États fédérés (5). En outre, aux termes de la section 2 b) de cette loi, aucune loi fédérale ne peut abroger ou altérer la réglementation d'un État fédéré ni s'y substituer, «à moins qu'une telle loi ne se rapporte expressément aux activités d'assurance» [15 USC, § 1012 b)]. Toutefois, les dispositions de la loi sur la FTC s'appliquent au secteur de l'assurance «dans la mesure où cette activité n'est pas réglementée par les États fédérés» (*idem*). Par ailleurs, il convient de noter que la loi McCarran-Ferguson n'attribue la compétence aux États fédérés que pour ce qui concerne les «activités d'assurance». De ce fait, la FTC reste compétente, à titre supplétif, pour les manœuvres et pratiques déloyales ou frauduleuses auxquelles se livrent les compagnies d'assurances dans le cadre d'activités ne relevant pas du secteur de l'assurance. Tel pourrait, par exemple, être le cas lorsque des assureurs vendent

(1) Le 12 novembre 1999, le président Clinton a rendu exécutoire, par sa signature, la loi Gramm-Leach-Bliley (Pub. L. 106-102, codifiée sous 15 USC, § 6801 et suivantes). Cette loi limite la divulgation, par les établissements financiers, d'informations à caractère personnel relatives à leurs clients. Elle leur impose, entre autres, d'informer tous les clients de leurs principes et pratiques destinés à protéger la vie privée dans le cadre du partage des informations à caractère personnel avec des entreprises affiliées ou on. La loi autorise 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. Les organismes publics concernés ont émit des propositions de disposition à cette fin.

(2) Par sa fomulation, cette dérogation ne vaut pas pour le secteur des valeurs mobilières. Les courtiers, les opérateurs sur titres et les autres acteurs de ce secteur relèvent, par conséquent, de la compétence concurrente de la Securities and Exchanges Commission et de la FTC en ce qui concerne les manœuvres et pratiques déloyales ou frauduleuses.

(3) La dérogation prévue à la section 5 mentionnait initialement le Federal Home Loan Bank Board, qui a été supprimé par le Financial Institutions Reform, Recovery and Enforcement Act de 1989. Les fonctions de cet organe ont été transférées à l'Office of Thrift Supervision ainis qu'à la Resolution Trust Corporation, à la Federal Deposit Insurance Corporation et au Housing Finance Board.

(4) Bien qu'elle fasse sortir les établissements financiers du domaine de compétence de la FTC, la section 5 dispose également que, chaque fois que la FTC édictera une règle relative aux manœuvres et pratiques déloyales ou frauduleuses, les organes chargés de la réglementation financière devront adopter des dispositions analogues dans un délai de soixante jours [15 USC, § 57 a) f) 1)].

(5) «Les activités d'assurance ainsi que toute personne exerçant ce genre d'activités sont soumises aux lois des différents États fédérés relatives à la réglementation ou à l'imposition de ces activités» [15 USC, § 2012 a)].

▼B

des informations à caractère personnel sur leurs souscripteurs à des sociétés de vente directe de produits étrangers au secteur de l'assurance (1).

Transporteurs publics

La deuxième dérogation prévue à la section 5 concerne les transporteurs publics «soumis aux lois visant à réglementer le commerce» [15 USC, § 45 a) 2)]. Dans le cas présent, les «lois visant à réglementer le commerce» correspondent au sous-titre IV du titre 49 du United States Code et au Communications Act de 1934 (47 USC, § 151 et suivantes) [15 USC, § 44].

Le sous-titre IV du titre 49 du USC («Transport inter-États») couvre les transporteurs par voie ferrée, par route et par voie navigable, les fréteurs, les commissionnaires de transport et les transporteurs par pipelines (49 USC, § 10101 et suivantes). Ces divers transporteurs publics sont soumis à la réglementation arrêtée par le Surface Transportation Board, un organisme indépendant relevant du ministère des transports (49 USC, §§ 10501, 13501 et 15301). Dans tous les cas, il est interdit au transporteur de divulguer des informations sur la nature, la destination et d'autres aspects du fret transporté qui pourraient être utilisées au détriment de l'expéditeur (49 USC, §§ 11904, 14908 et 16103). Il est à noter que ces dispositions se réfèrent aux informations concernant le fret de l'expéditeur et qu'elles ne semblent donc pas s'étendre aux données personnelles de l'expéditeur ne se rapportant pas aux marchandises expédiées.

Le Communications Act prévoit que le «commerce inter-États et international des communications par fil et par ondes radioélectriques» est réglementé par la Federal Communications Commission (FCC) (47 USC, §§ 151 et 152). Cette loi s'applique non seulement aux entreprises de télécommunications publiques, mais également à d'autres entreprises, telles que les télédiffuseurs, les radiodiffuseurs et les fournisseurs de services par câble, qui ne sont pas des transporteurs publics et qui ne remplissent donc pas les conditions requises pour bénéficier de la dérogation prévue à la section 5 de la loi sur la FTC. Par conséquent, la FTC est compétente pour examiner si ces dernières entreprises se livrent à des pratiques déloyales et frauduleuses, tandis que la FCC possède une compétence concurrente lui permettant d'exercer des pouvoirs indépendants dans ce domaine, ainsi qu'il est décrit ci-après.

Aux termes du Communications Act, «toute société de télécommunications», y compris les compagnies locales, est tenue de protéger la confidentialié de ses informations exclusives sur les clients (2) [47 USC, § 222 a)]. En plus de cette disposition générale en matière de protection de la vie privée, le Communications Act a été modifié par le Cable Communications Policy Act de 1984 (dit «Cable Act») (47 USC, § 521 et suivantes), afin de prescrire que les câblo-opérateurs protègent la confidentialité des «informations personnellement identifiables» sur les abonnés au câble (47 USC, § 551) (3). Le Cable Act restreint la collecte d'informations à caractère personnel par les câblo-opérateurs et fait obligation à ces derniers d'informer les abonnés de la nature et de l'utilisation ultérieure des informations collectées. Il accorde aux abonnés le droit d'accéder aux informations les concernant et impose aux câblo-opérateurs de détruire ces informations dès lors qu'elles ne leur sont plus nécessaires.

(1) La FTC a fait usage de ses pouvoirs à l'égard des compagnies d'assurances dans différents contextes. Dans l'un des cas, elle a pris des mesures contre une entreprise ayant fait de la publicité mensongère dans un État fédéré où elle n'était pas agréée. La compétence de la FTC a été confirmée au motif qu'il n'existait aucune réglementation efficace au niveau fédéré, puisque l'entreprise était, en fait, hors de portée de l'État en question. Voir [FTC Trayelers Health Association, 362 US 293 (1960)].
En ce qui concerne les États fédérés, dix-sept d'entre eux ont adopté la loi type sur la protection des informations et de la vie privée dans le secteur de l'assurance (Insurance Information and Privacy Protection Act), élaborée par la National Association of Insurance Commissioners (NAIC). Cette loi comprend des dispositions relatives à l'information des assurés, à l'utilisation et à la divulgation des données collectées ainsi qu'à l'accès à ces dernières. Par ailleurs, la quasi-totalité des États fédérés ont adopté la loi type sur les pratiques d'assurance déloyales (Unfair Insurance Practices Act), élaborée par la NAIC, qui vise expressément les pratiques commerciales déloyales dans le secteur de l'assurance.

(2) L'expression «informations de réseau exclusives sur les clients» (*customer proprietary network information*) désigne les informations concernant «le nombre, la configuration technique, le type, la destination et la fréquence d'utilisation des services de télécommunications» fournis à un client ainsi que les informations contenues dans les factures de téléphone [47 USC, § 222 f) 1)]. Elle n'englobe toutefois pas les informations relatives à la liste des abonnés (*idem*).

(3) La loi ne définit pas expressément la notion d'«information personnellement identifiable» (*personally identifiable information*).

▼B

Le Communications Act donne compétence à la FCC pour mettre en œuvre — de sa propre initiative ou en réponse à une plainte extérieure — ces deux dispositions relatives à la confidentialité [1] (47 USC, §§ 205, 403; § 208). Si la FCC établit qu'une société de télécommunications (y compris un câblo-opérateur) a violé les règles de confidentialité énoncéesaux sections 222 ou 551, elle peut, fondamentalement, prendre tois mesures différentes. Après avoir procédé à une audition et constaté la violation, elle peut, tout d'abord, ordonner au transporteur de payer des dommages-intérêts [2] (47 USC, § 209). Au lieu de cela, elle a également la possibilité d'adresser une ordonnance de cessation au transporteur, afin qu'il mette fin à la pratique ou à l'omission incriminée [47 USC, § 205 a)]. Enfin, la FCC peut aussi ordonner à un transporteur contrevenant de «se conformer à toute réglementation ou pratique» susceptible d'être prescrite par la FCC (idem).

Les particuliers qui estiment qu'une société de télécommunications ou un câblo-opérateur a violé les dispositions correspondantes du Communications Act ou du Cable Act peuvent soit déposer une plainte auprès de la FCC, soit saisir un tribunal fédéral de première instance (47 USC, § 207). Les plaignants qui obtiennent gain de cause lors d'un procès intenté, devant un tribunal fédéral, à une société de télécommunications pour manquement à l'obligation de protéger les informations exclusives sur les clients dans le cadre général de la section 222 du Communications Act peuvent bénéficier de la réparation du préjudice effectivement subi et du remboursement de leurs frais d'avocat (47 USC, § 206). Les plaignants qui engagent des poursuites en alléguant une violation de la confidentialité dans le cadre spécifique de la section 551 du Cable Act peuvent se voir accorder, en sus, des dommages-intérêts à titre de sanction et la prise en charge, dans des limites raisonnables, des dépenses [47 USC, § 551 f)].

La FCC a fixé les modalités d'application de la section 222 (47 CFR, 64.2001-2009). Ces règles détaillées énumèrent un certain nombre de mesures de sauvegarde destinées à protéger les informations de réseau exclusives sur les clients contre tout accès non autorisé. Elles font obligation aux sociétés de télécommunications:

— de développer et de mettre en œuvre des systèmes logiciels indiquant la situation vis-à-vis du client (information/consentement) lorsque son dossier apparaît pour la première fois à l'écran,

— de conserver une «piste de contrôle» électronique afin de retracer les accès à un compte client, et notamment de déterminer quand, par qui et dans quel but le dossier d'un client est consulté,

— de former leur personnel à l'utilisation autorisée des informations de réseau exclusives sur les clients et de mettre en place des procédures disciplinaires appropriées,

— d'instaurer un processus de révision et de surveillance afin de garantir le respect des règles lors de l'exercice d'activités de *marketing* externe,

— de déclarer annuellement à la FCC les mesures prises pour se conformer à ces règles.

Transporteurs aériens

Les transporteurs aériens — tant américains qu'étrangers — soumis au Federal Aviation Act de 1958 sont également exclus du champ d'application de la section 5 du FTC Act [15 USC, § 45 a) 2)]. Est concernée toute personne fournissant des services de transport inter-États ou international de marchandises ou de passagers par avion, ou transportant du courrier par avion (49 USC, § 40102). Les transporteurs aériens relèvent de la compétence du ministère des transports. De ce fait, le ministre des transports est autorisé à prendre des mesures «empêchant les pratiques déloyales, frauduleuses, abusives ou anticoncurrentielles dans le secteur du transport aérien» [49 USC, § 40101 a) 9)]. Dès lors que l'intérêt public l'exige, il peut examiner si un transporteur aérien américain ou étranger, ou un agent délivrant des billets d'avion, s'est livré à une pratique déloyale ou frauduleuse (49 USC ,§ 41712). Après une audition, il peut rendre une ordonnance visant à faire cesser la pratique illégale en question (*idem*). À notre connaissance, le ministre des transports n'a pas encore fait usage de ces pouvoirs en relation avec la

[1] Cette compétence comprend, notamment, le droit de demander réparation du préjudice subi en cas de violations de la confidentialité au regard de la section 222 du Communications Act et, pour les abonnés au câble, de la section 551 du Cable Act modifiant le Communications Act [voir également 47 USC, § 551 f) 3)] (une action civile devant un tribunal fédéral de première instance constitue un recours non exclusif, disponible «en complément de toute autre voie de droit ouverte à un abonné au câble»).

[2] Toutefois, l'absence de dommage direct pour un plaignant ne peut pas être invoquée pour rejeter une plainte. [47 USC, § 208 a)].

▼B

protection de la confidentialité des informations à caractère personnel sur les clients des compagnies aériennes [1].

Deux dispositions protégeant la confidentialité des informations à caractère personnel sont applicables aux transporteurs aériens dans des contextes spécifiques. D'une part, le Federal Aviation Act protège la vie privée des candidats à un poste de pilote [49 USC, § 44936 f)]. Bien qu'elle autorise les transporteurs aériens à se procurer des renseignements sur les antécédents professionnels d'un candidat, cette loi donne au candidat le droit d'être averti de la demande de tels renseignements, de donner son consentement à cette demande, de corriger les inexactitudes et de ne voir divulguer ces renseignements qu'aux seules personnes participant à la décision de recrutement. D'autre part, la réglementation du ministère des transports exige que les informations de la liste de passagers, collectées à des fins administratives, dans l'éventualité d'une catastrophe aérienne, soient «traitées de manière confidentielle et communiquées uniquement au ministère américain des affaires étrangères, au National Transportation Board (à la demande du NTSB) et au ministère américain des transports» [14 CFR, partie 243, § 243.9 c)] (ajouté par 63 FR 8258).

Conditionneurs et exploitants de parcs à bestiaux

Le Packers and Stockyards Act (loi sur les conditionneurs et les exploitants de parcs à bestiaux) de 1921 (7 USC, § 181 et suivantes), interdit à «tout conditionneur d'animaux, de viande, de produits alimentaires à base de viande ou de produits animaux non manufacturés, et à tout négociant en volailles vivantes de se livrer ou de recourir, dans le cadre de ses activités, à des pratiques ou manœuvres déloyales, injustement discriminatoires ou frauduleuses» [7 USC, § 192 a); voir également 7 USC, § 213 a)] (interdisant «toute pratique ou manœuvre déloyale, injustement discriminatoire ou frauduleuse» en relation avec les animaux). La responsabilité de la mise en œuvre de ces dispositions incombe principalement au ministre de l'agriculture, la FTC restant compétente pour le commerce de détail et les opérations concernant l'industrie des volailles [7 USC, § 227 b) 2)].

Il n'est pas certain que le ministre de l'agriculture interprétera le fait, pour un conditionneur ou un exploitant de parc à bestiaux, de ne pas protéger la vie privée des personnes conformément à sa politique déclarée en la matière comme une pratique «frauduleuse» au sens du Packers and Stockyards Act. Toutefois, la dérogation de la section 5 ne s'applique aux personnes, aux sociétés de personnel et aux sociétés anonymes que «dans la mesure où celles-ci sont soumises au Packers and Stockyards Act». Par conséquent, si la protection de la vie privée n'entre pas dans le champ du Packers and Stockyards Act, la dérogation prévue à la section 5 peut très bien ne pas s'appliquer et les conditionneurs, ainsi que les exploitants de parcs à bestiaux relèveraient donc à cet égard de la compétence de la FTC.

Pouvoirs des États fédérés en matière de «pratiques déloyales et frauduleuses»

D'après une analyse réalisée par les services de la FTC, «les cinquante États américains ainsi que le District of Columbia, Guam, Porto Rico et les îles Vierges ont adopté des lois plus ou moins similaires au Federal Trade Commission Act afin de lutter contre les pratiques déloyales ou frauduleuses». [«FTC fact shet», réimprimé dans *Comment, Consumer Protection*: «The Practival Effectiveness of State Deceptive Trade Practices Legislation», 59 Tul. L. Rev. 427 (1984)]. Dans tous les cas, un organisme public chargé de la mise en œuvre de la législation est habilité à mener des enquêtes par l'émission de citations à comparaître sous peine de sanction ou de demandes d'enquêtes au civil, à obtenir des organisations concernées l'assurance qu'elles respectent volontairement la législation, à émettre des ordonnances de cessation et à solliciter des injonctions en vue d'empêcher le recours à des pratiques commerciales déloyales, indélicates ou frauduleuses (*idem*). Sur quarante-six des territoires précités, la loi permet aux particuliers d'intenter des actions visant à obtenir une indemnisation simple, double ou triple, ou encore des indemnités à titre de sanction ainsi que, dans certains cas, le remboursement des dépens et des frais d'avocat (*idem*).

[1] Il semble que des efforts soient actuellement entrepris dans cette branche d'activité pour traiter le problème de la protection de la vie privée. Les représentants de la branche ont examiné les principes proposés pour la «sphère de sécurité» et leur application éventuelle aux transporteurs aériens. Cet examen a également englobé une proposition visant à adopter une politique de protection de la vie privée valable pour l'ensemble de la branche et dans le cadre de laquelle les entreprises participantes se soumettraient expressément à l'autorité du ministère des transports.

▼B

Le Deceptive and Unfair Trade Practices Act de l'État de Floride autorise, par exemple, le procureur général (*attorney general*) à enquêter et à intenter des actions civiles pour «concurrence déloyale ou pratiques commerciales déloyales, indélicates ou frauduleuses», englobant la publicité mensongère ou trompeuse, les offres fallacieuses de franchises ou d'opérations commerciales, les pratiques de télémarketing frauduleuses et les systèmes de vente pyramidale. Voir également NY General Business Law § 349 (interdisant les actes déloyaux et les pratiques frauduleuses dans le monde des affaires).

Une enquête réalisée cette année par la National Association of Attorneys General (NAAG) confirme ces indications. Chacun des quarante-trois États à avoir répondu à des dispositions instituent une «mini-FTC» ou garantissent une protection comparable. Toujours selon cette enquête, trente-neuf États se disent compétents pour examiner des plaintes déposées par des non-résidents. En ce qui concerne la protection de la vie privée des consommateurs, en particulier, trente-sept des quarante et un États à avoir répondu indiquent qu'ils donneraient suite à des plaintes alléguant qu'une entreprise établie sur leur territoire n'adhérerait pas à ses propres déclarations en matière de protection de la vie privée.

▼B

ANNEXE IV

Confidentialité et dommages-intérêts, autorisations légales et fusions et acquisitions suivant la législation des États-Unis

Le présent document répond à la demande de la Commission européenne visant à la clarification de la législation américaine en ce qui concerne a) les demandes de compensations pour violations de la confidentialité, b) «les autorisations explicites» prévues par la légisaltion américaine pour utilisation d'informations à caractère personnel d'une façon contredisant les principes de la «sphère de sécurité» et c) l'effet des fusions et acquisitions sur les obligations contractées conformément aux principes de la sphère de sécurité.

A. **Compensations pour violations de la confidentialité**

Le non-respect des principes de la «sphère de sécurité» pourrait donner lieu à un certain nombre de réclamations suivant les circonstances. En particulier, les organisations de la «sphère de sécurité» pourraient être taxées de présentation erronée pour n'avoir pas respecté leurs politiques déclarées en matière de confidentialité. Les particuliers peuvent également entreprendre des actions juridiques en vue d'obtenir réparation de violations de la confidentialité. De nombreuses dispositions sont prévues aux nivaux fédéral et national pour instruire les demandes en réparation introduites par les particuliers en cas de violation.

Le droit à réparation pour atteinte à la vie privée est bien établi par la législation américaine.

Diverses théories juridique stipulent que l'usage des données à caractère personnel d'une manière incompatible avec les principes de la «sphère de sécurité» peut entraîner une responsabilité légale. Par exemple, aussi bien le maître de fichier qui transfère des données que les personnes concernées pourraient poursuivre l'organisation relevant de la «sphère de sécurité» qui manquerait à ses engagements de «sphère de sécurité» en cas de présentation erronée. Selon le Restatement of the Law, Second Torts ([1]):

> Quinconque se rend coupable d'une présentation erronée relative à des faits, des opinions, des intentions ou une loi en vue d'inciter une autre personne à agir ou à s'abstenir d'agir sur la foi de cette déclaration endosse la responsabilité des éventuelles pertes pécuniaires subies par cette personne du fait du crédit qu'elle aura jugé bon d'attacher à ladite présentation.

(Restatement, alinéa 525). Une présentation erronée est réputée «frauduleuse» si celle-ci est faite sciemment *idem*, alinéa 526). En règle générale, quiconque fait sciemment une présentation erronée est potentiellement responsable vis-à-vis de ceux qui encourront une perte pécuniaire du fait qu'ils se seront fiés à cette déclaration (*idem*, alinéa 531). De surcroît, quiconque fait sciemment une présentation erronée à autrui peut être considéré comme responsable vis-à-vis d'un tiers si le déclarant s'attend que sa présentation erronée sera répétée à un tiers qui y ajoutera foi (*idem*, alinéa 533).

Dans le cadre de la «sphère de sécurité», la représentation pertinente est la déclaration publique par laquelle l'organisation atteste que celle-ci adhérera aux principes de la sphère de sécurité. Une fois pris un tel engagement, le non-respect délibéré de ces principes pourrait donner motif à engager une procédure en présentation erronée de la part de ceux qui y auraient accordé crédit. Étant donné que l'engagement de respecter ces principes est universel, les personnes concernées par cette information ainsi que le maître de fichier européen transférant des informations à caractère personnel à l'organisation des États-Unis pourraient se retourner contre l'organisation américaine en cas de présentation erronée ([2]). De plus, l'organisation américaine demeure responsable vis-à-vis de ces personnes pour «présentation erronée rétiérée» tant que ces personnes s'en remettent à leur détriment à cette présentation erronée (Restatement, alinéa 535).

Quiconque s'en remet à une présentation erronée a droit à obtenir des dommages-intérêts. Selon le Restatement:

> Le destinataire d'une présentation erronée est habilité à récupérer sous forme de dommages-intérêts la perte pécuniaire que l'auteur de la présentation aurait juridiquement entraînée à son encontre.

([1]) Second Restatement of the Law — Torts; American Law Institute (1997).

([2]) Tel pourrait être, par exemple, le cas lorsque les personnes s'en sont remises aux engagements de l'organisation américaine en matière de sphère de sécurité pour consentir à ce que le maître de fichier transfère leurs données nominatives aux États-Unis.

▼B

(Restatement, alinéa 549). Ces dommages-intérêts comprennent, outre les pertes pécuniaires, le «manque à gagner» d'une opération commerciale [*idem*; voir, par exemple, Boling v. Tennessee State Bank, 890 S.W.2d 32 (1994)] (la banque doit indemniser les emprunteurs à hauteur de 14 825 dollars pour avoir divulgué des informations nominatives ainsi que des *business plan* des emprunteurs au président de la banque qui avait un intérêt contradictoire):

Étant donné que la présentation erronée implique une connaissance effective ou du moins la conviction que la présentation est erronée, la responsabilité peut également s'attacher à la présentation erronée par négligence. D'après le Restatement, quiconque fait une présentation erronée dans l'exercice de son métier, de sa profession ou de son emploi, ou à l'occasion d'une opération financière peut être tenu responsable «faute d'exercer la prudence ou la compétence raisonnable dans l'obtention ou la communication de l'information» [Restatement, alinéa 552 1)]. Contrairement aux déclarations frauduleuses, les dommages-intérêts en cas de présentation erronée par négligence sont limités aux pertes pécuniaires [*idem*, alinéa 552 B 1)].

Dans une affaire récente, par exemple, la cour d'appel du Connecticut a jugé que le fait qu'une entreprise fournisseuse d'électricité ait omis de déclarer qu'elle avait transmis des informations relatives au paiement de la clientèle à des organismes de crédit nationaux constituait le motif d'une instance en justice pour présentation erronée (voir Brouillard v. United Illuminating Co., 1999 Conn. Super. LEXIS 1754). Dans cette affaire, la partie plaignante s'est vu opposer un refus de crédit du fait que le défendeur avait fait état de retards de paiement pour factures non honorées dans les trente jours. Le plaignant a fait valoir qu'il n'avait pas été informé de cette politique lorsqu'il avait souscrit un abonnement de fourniture électrique à caractère résidentiel auprès du défendeur. La cour a jugé plus particulièrement qu'«une plainte pour présentation erronée par négligence peut s'appuyer sur l'absence de déclaration du défendeur lorsque celui-ci en a l'obligation». Cette affaire démontre également que le fait d'agir «à bon escient» ou l'intention frauduleuse ne constitue pas un élément nécessaire comme motif de former une demande en justice pour présentation erronée des faits par négligence. Ainsi, une organisation américaine qui néglige de divulguer intégralement la façon dont elle utilisera des informations à caractère personnel reçues selon les principes de la sphère de sécurité pourrait être tenue pour responsable de présentation erronée des faits.

Dans la mesure où une violation des principes de la sphère de sécurité a entraîné un usage abusif d'informations à caractère personnel, la personne concernée pourrait être fondée par ailleurs à introduire une plainte pour le délit d'atteinte à la vie privée, reconnu par la *common law*. Le droit américain reconnaît depuis longtemps les motifs d'actions liés aux infractions à la vie privée. Dans une affaire remontant à 1905 ([1]), la Cour suprême de Géorgie a établi que le droit à la protection de la vie privée s'enracinait dans les principes de la *natural law* et de la *common law* en statuant sur le cas d'un citoyen dont la photographie avait été utilisée par une société d'assurance vie, à l'insu de ce dernier et sans son consentement, pour illustrer une publicité commerciale. Énonçant des thèmes désormais familiers de la jurisprudence américaine en matière de vie privée, le tribunal a jugé que l'utilisation de la photographie était «délictueuse», «malveillante», et tendait à «ridiculiser le plaignant aux yeux du monde entier» ([2]). Les fondements du jugement Pavesich ont prévalu, avec des variations mineures, pour devenir le socle du droit américain en la matière. Les tribunaux d'État ont en permanence soutenu les actions intentées dans le domaine des atteintes à la vie privée, et ils sont au moins quarante-huit États à reconnaître à présent le bien-fondé judiciaire de telles actions ([3]). De surcroît, au moins douze États disposent de dispositions constitutionnelles sauvegardant le droit de leurs citoyens contre les actes d'intrusion dans leur vie privée ([4]), lesquelles pourraient, dans certains cas, être étendues à la protection contre les instrusions qui seraient commises par des entités non gouvernementales [voir, par exemple, Hill v. NCAA, 865 P.2d 633 (Ca. 1994); voir également S. Ginder, Lost and Found in Cyberspace: Informational Privacy in the Age of the Internet, 34 S.D. L. Rev. 1153 (1997)]. («Les Constitutions de certains États prévoient des protections de la vie privée qui vont au-delà des dispositions analogues dans la Constitution fédérale. L'Alaska, l'Arizona, la Californie, la Floride, Hawaii, l'Illinois, la

([1]) Pavesich v. New England Life Ins. Co., 50 S.E. 68 (Ga. 1905).

([2]) *Idem*, 69.

([3]) Une consultation électronique de la base de données Westlaw a recensé 2 703 plaintes intentées auprès de tribunaux d'État qui relevaient de «la vie privée» depuis 1995. Nous avons déjà transmis à la Commission les résultats de cette recherche.

([4]) Voir, par exemple, Alaska Constitution, Art. 1, Sec. 22; Arizona, Art. 2, Sec. 8; California, Art. 1, Sec. 1; Florida, Art. 1, Sec. 23; Hawaii, Art. 1, Sec. 5; Illinois, Art. 1, Sec. 6; Louisiana, Art. 1, Sec. 5; Montana, Art.2, Sec. 10; New York, Art. 1, Sec. 12; Pennsylvania, Art. 1, Sec. 1; South Carolina, Art. 1, Sec. 10; and Washington, Art. 1, Sec. 7.

▼B

Louisiane, le Montana, la Caroline du Sud et l'État de Washington disposent d'un arsenal plus large de protection de la vie privée.»).

Le Second Restatement of Torts livre un panorama faisant autorité du droit dans ce domaine. Reflétant la procédure juridique commune, le Restatement explique que le «droit à la protection de la vie privée» englobe sous cette dénomination générique quatre possibilités distinctes de poursuites pour délits, (voir Restatement, alinéa 652A). En premier lieu, une plainte pour «intrusion dans la solitude» est recevable contre un défendeur qui porte intentionnellement atteinte,par voie physique ou autre, à la solitude ou à l'isolement d'une autre personne ou à ses affaires ou intérêts privés (1). En second lieu, une plainte pour «usurpation» peut être introduite lorsqu'une personne s'approprie le nom ou l'apparence d'une autre personne à ses propres fins (2). Troisièmement, la «publication de faits privés» est passible de poursuites lorsque la circonstance divulguée est de nature à porter gravement préjudice à une personne raisonnable et ne revêt pas le caractère de préoccupation publique légitime (3). Enfin, une action pour «publicité mensongère» est légitime lorsque le défendeur place sciemment ou imprudemment autrui sous un jour public fallacieux susceptible de porter le plus grand tort à une personne raisonnable (4).

Dans le cadre de la «sphère de sécurité», «l'ingérence dans la sphère privée» pourrait englober la collecte non autorisée d'informations à caractère personnel, tandis que l'utilisation non autorisée d'informations à caractère personnel à des fins commerciales pourrait donner lieu à une instance d'appropriation. De la même façon, la divulgation d'informations personnelles inexactes ferait l'objet d'un délit de «publicité mensongère» si l'information s'avère être hautement préjudiciable à une personne raisonnable. Enfin, l'atteinte à la vie privée résultant de la publication ou de la divulgation d'informations personnelles sensibles pourrait donner matière à poursuite pour «publication de faits privés» (voir exemples illustrés ci-dessous).

Pour ce qui est de la question des dommages-intérêts, les atteintes à la vie privée ouvrent droit à dédommagements à la personne lésée pour ce qui est:

a) du préjudice occasionné à sa vie privée résultant de cette atteinte;

b) du préjudice psychologique avéré subi, si ce dernier est de nature normalement attribuable à une telle atteinte

c) et, enfin, de tout préjudice particulier dont ladite atteinte serait une cause légale.

(Restatement, alinéa 652 H). Étant donné l'application générale de la législation en matière de délits et la multiplicité des plaintes recevables pour ce qui est des différents aspects des intérêts liés à la vie privée, les dédommagements financiers sont susceptibles d'être accordés à quiconque verrait mis en cause des intérêts liés à sa vie privée suite au non-respect des principes dits de la «sphère de sécurité».

De fait, les tribunaux d'État ne comptent plus les plaintes pour atteinte à la vie privée dans des situations analogues. Ex parte AmSouth Bancorporation et al., 717 So. 2d 357, par exemple, impliquait une action en justice d'une portée générale selon laquelle le défendeur «avait exploité les déposants de fonds fiduciaires de la banque, en partageant des informations confidentielles concernant lesdits déposants et leurs comptes» pour permettre à un affilié de la banque de vendre des fonds de placement et d'autres investissements. Des dommages-intérêts sont souvent accordés dans de tels cas. Dans l'affaire Vassiliades v. Garfinckel's, Brooks Bros., 492 A.2d 580 (DC App. 1985), une cour d'appel a infirmé le jugement d'une cour inférieure pour conclure que l'utilisation de photographies de la partie plaignante «avant» et «après» une intervention de chirurgie plastique, lors d'une présentation effectuée dans un grand magasin, constituait une atteinte à la vie privée du fait de la publication de faits privés. Dans l'affaire Candebat v. Flanagan, 487 So.2d 207 (Miss. 1986), la compagnie d'assurances du défendeur a utilisé un accident au cours duquel l'épouse du plaignant fut gravement blessée pour une campagne publicitaire. Le plaignant a introduit une action pour atteinte à la vie privée. Le tribunal a estimé que le plaignant pouvait obtenir réparation pour détresse émotionnelle et appropriation d'identité. Les plaintes pour appropiration frauduleuse peuvent être instruites même si le plaignant n'est pas célèbre personnellement [voir, par exemple, Staruski v. Continental Telephone C., 154 Vt. 568 (1990)] (le défendeur a tiré un profit commercial de l'utilisation du nom et de la photographie d'un salarié dans une annonce parue dans un journal). Dans l'affaire Pulla v. Amoco Oil Co., 882 F. Supp. 836 (SD Iowa 1995), un employeur a porté atteinte à la «sphère privée» d'un salarié plaignant en faisant vérifier par un autre employé les extraits de cartes de crédit de celui-ci de manière à retracer les absences pour maladie. La cour a octroyé 2 dollars de dommages-intérêts,

(1) *Idem*, chapitre 28, paragraphe 652 B.
(2) *Idem*, chapitre 28, paragraphe 652 C.
(3) *Idem*, chapitre 28, paragraphe 652 D.
(4) *Idem*, chapitre 28, paragraphe 652 E.

▼B

assortis de 500 000 dollars de pénalités pour réparation de préjudice moral. Un autre employeur fut tenu responsable pour avoir publié dans le journal d'entreprise l'histoire d'un salarié mis à pied pour avoir soi-disant falsifié ses états de service [voir Zinda v. Louisiana-Pacific Corp., 140 Wis.2d 277 (Wis.App. 1987)]. Les faits relatés portaient atteinte à la vie privée du plaignant du fait qu'il s'agissait de la publication d'une affaire privée, mais que le journal était diffusé parmi les collègues de travail. Enfin, un collège qui avait pratiqué sur ses étudiants le test du sida après avoir prétendu que le test sanguin ne concernait que la rubéole fut jugé responsable d'atteinte à la «sphère privée» [voir Doe v. High-Tech Institute, Inc., 972 P.2d 1060 (Colo. App. 1998)]. (Pour les autres cas cités, voir Restatement, alinéa 652 H, annexe.)

Les États-Unis sont souvent critqués pour la part trop belle faite aux plaideurs, mais cela à pour corollaire que les individus ont accès aux voies légales et ne se privent pas d'utiliser celles-ci lorsqu'ils estiment avoir été victimes d'un préjudice.De nombreux aspects du système judiciaire américain font qu'il est facile au plaignant d'intenter un procès, individuellement ou en tant que groupe. Le barreau, plus nombreux que dans la plupart des autres pays, fait que la représentation professionnelle est facilement disponible. L'avocat de la partie civile, représentant les particuliers dans les procès privés, fixe normalement ses honoraires sur une base aléatoire, ce qui permet même aux plus démunis d'obtenir réparation. Il s'agit là d'un facteur important — aux États-Unis, chaque partie débourse normalement ses propres frais d'avocat et autres dépenses. Ce système est à l'opposé de la règle européenne qui veut que la partie perdante rembourse à l'autre partie les frais exposés. Sans débattre des mérites relatifs des deux systèmes, force est d'admettre que la règle américaine paraît moins de nature à décourager les procès intentés par des personnes qui ne seraient pas en mesure de faire face aux coûts des deux parties au cas où elles perdraient leur procès.

Les individus peuvent intenter un procès même si leurs revendications sont relativement modestes. La plupart des juridictions américaines, sinon toutes, disposent de tribunaux inférieurs garantissant des procédures simplifiées et moins onéreuses dans le cas des différends se situant en deçà des limites fixées par la loi ([1]). La possibilité de pénalités pour réparation d'un préjudice moral offre également une compensation financière aux personnes ayant subi un léger préjudice direct et qui engagent un procès contre une conduite répréhensible. Enfin, les personnes s'estimant lésées solidairement peuvent faire bourse et cause communes en introduisant une action en justice d'une portée générale.

Un bon exemple de la capacité des individus à intenter un procès en réparation est représenté par le contentieux en cours contre Amazon.com pour atteinte à la vie privée. Amazon.com, le grand détaillant en ligne, est la cible d'une action en justice de portée générale, dans laquelle les plaignants font valoir qu'ils n'ont pas été informés de la collecte d'informations personnelles les concernant et n'ont pas donné leur accord à la collecte de ces informations lorsqu'ils utilisaient un programme logiciel propriété d'Amazon et dénommé «Alexa». Dans cette affaire, les plaignants ont invoqué des violations du Computer Fraud and Abuse Act sous la forme d'un accès illicite à leurs communications enregistrées ainsi que de l'Electronic Communications Privacy Act pour interception illicite de leurs communications électroniques et téléphoniques. Ils ont également invoqué une atteinte à la vie privée au titre de la *common law.* Cette action découle d'une plainte introduite par un expert en sécurité Internet en décembre. La demande en réparation s'élève à 1 000 dollars par personne, majorés des honoraires d'avocat et des bénéfices encourus suite à la violation de la législation. L'action touchant des millions de personnes, les dommages-intérêts pourraient s'élever à des milliards de dollars. La FTC (Federal Trade Commission) examine elle aussi les chefs d'accusation.

La législation fédérale et nationale sur la vie privée offre souvent des motifs privés d'actions en matière de préjudice financier

Outre qu'elle donne lieu à une responsabilité civile en matière de droit des délits, la non-conformité aux principes de la «sphère de sécurité» pourrait également contrevenir à l'une ou l'autre des centaines de lois fédérales et nationales en matière de protection de la vie privée. Beaucoup de ces lois, qui concernent le traitement des informations à caractère personnel aussi bien par les organismes gouvernementaux que par le secteur privé, autorisent les poursuites en dommages-intérêts lorsque les individus sont victimes de violations.

Electronic Communications Privacy Act de 1986. L'ECPA interdit l'interception non autorisée de communications téléphoniques cellulaires et de transmission d'ordinateur à ordinateur. Les violations peuvent entraîner une responsabilité civile d'au moins 100 dollars par journée de violation. La protection de l'ECPA s'étend également à l'accès non autorisé ou à la divulgation de communications

([1]) Nous avons déjà fourni à la Commission des informations sur les procès se tenant dans les instances inférieures.

▼B

électroniques enregistrées. Les contrevenants sont responsables des préjudices occasionnés ou de la perte de profit entraînée par une violation.

Telecommunications Act de 1996. Conformément au paragraphe 702, les informations sur le réseau homogène client (CPNI) ne peuvent être utilisées dans un objectif autre que celui de fournir des services de télécommunication. Les abonnés au service ont la possibilité soit de présenter une plainte à la Federal Communications Commission, soit d'engager des poursuites devant le tribunal de district fédéral en vue de l'obtention de dommages-intérêts et de la restitution des honoraires d'avocat.

Consumer Credit Reporting Reform Act de 1996. La loi de 1996 a modifié le Fair Credit Reporting Act de 1970 (FCRA) pour exiger l'amélioration de l'information et du droit d'accès des assujettis aux crédits. Le Reform Act imposait également de nouvelles restrictions aux revendeurs d'informations sur les crédits à la consommation. Les consommateurs peuvent obtenir des dommages-intérêts et la restitution des honoraires d'avocat pour violation.

Les lois des États protègent également la vie privée dans une large gamme de situations. Parmi les domaines où les États ont pris des initiatives, on peut citer les relevés bancaires, les abonnements aux câblo-opérateurs, les informations en matière de crédits, les états de service en matière d'emplois, les archives administratives, l'information génétique et les dossiers médicaux, les informations en matière d'assurances, les dossiers scolaires, les communications électroniques et les locations vidéo [1].

B. **Autorisations légales explicites**

Les principes de la «sphère de sécurité» contiennent une exception lorsque le droit écrit, les réglementations ou la jurisprudence créent «des obligations conflictuelles ou des autorisations explicites, à condition que, dans l'exercice de ces autorisations, une organisation puisse démontrer que sa non-conformité aux principes est limitée dans la mesure nécessaire à la satisfaction des intérêts légitimes principaux favorisés par cette autorisation». Il est clair que lorsque la législation américaine impose une obligation conflictuelle, les organisations américaines faisant ou non partie de la «sphère de sécurité» doivent se plier à cette législation. Quant aux autorisations explicites, si les principes de la «sphère de sécurité» sont destinés à combler le fossé séparant les régimes américain et européen de protection de la vie privée, nous devons respecter les prérogatives législatives de nos législateurs élus. L'exception limitée au strict respect des principes de la «sphère de sécurité» s'efforce d'établir un équilibre pour tenir compte des intérêts légitimes de chaque partie.

L'exception est limitée aux cas où existe une autorisation explicite. Par conséquent, en tant que cas limite, la législation, la réglementation ou la décision de justice pertinente doivent autoriser affirmativement une conduite particulière des organisations adhérent à la «sphère de sécurité» [2]. En d'autres termes, l'exception ne s'appliquera pas lorsque la loi est silencieuse. De surcroît, l'exception ne s'appliquera que si l'autorisation explicite contredit le respect des principes de la «sphère de sécurité». Même dans ces conditions, l'exception «est limitée dans la mesure nécessaire à la satisfaction des intérêts légitimes principaux favorisés par cette autorisation». À titre d'illustration, lorsque la loi autorise simplement une société à fournir des informations à caractère personnel à des organismes gouvernementaux, l'exception ne s'appliquera pas. À l'inverse, lorsque la loi autorise spécifiquement la société à fournir des informations à caractère personnel à des organismes gouvernementaux sans le consentement de la personne, cela constituerait une «autorisation explicite» d'agir d'une manière contredisant les principes de la «sphère de sécurité». Par ailleurs, les exceptions spécifiques aux exigences de notification et de consentement entreraient dans le cadre de l'exception (car cela équivaudrait à une autorisation spécifique de révéler l'information sans notification et consentement). Par exemple, un texte de loi autorisant les médecins à fournir les dossiers médicaux de leurs patients aux fonctionnaires sanitaires sans l'autorisation préalable de ces patients pourrait permettre une exception aux principes de notification et de choix. Cette autorisation ne laisserait pas la possibilité à un médecin de fournir les mêmes dossiers médicaux aux caisses de maladie ou aux laboratoires de recherche pharmaceutique, car cela irait au-delà de l'objectif autorisé par la loi et donc

(1) Une récente interrogation électronique de la base de données Westlaw a recensé 994 affaires de dommages-intérêts et atteintes à la vie privée.

(2) Comme élément de clarification, l'autorité juridique pertinente ne devra pas faire spécifiquement référence aux principes de la «sphère de sécurité».

▼B

au-delà du champ de l'exception [1]. L'autorisation en question peut être une autorisation «autonome» de faire des choses déterminées avec des informations personnelles, mais, comme l'illustrent les exemples ci-dessous, il est plus probable qu'il s'agisse d'une exception à une loi plus large qui interdit la collecte, l'utilisation ou la divulgation d'informations à caractère personnel.

Telecommunications Act de 1996

Dans la plupart des cas, les utilisations autorisées sont conformes aux dispositions de la directive et aux principes, ou sont autorisés par l'une ou l'autre des exceptions admises. Par exemple, le paragraphe 702 du Telecommunications Act (codifié dans 47 USC, § 222) impose aux entreprises de télécommunications de maintenir la confidentialité des informations à caractère personnel obtenues durant la fourniture de leurs services aux clients. Cette disposition permet aux entreprises de télécommunications:

1) d'utiliser des informations clientèle pour fournir un service de télécommunications, et notamment la publication d'annuaires des abonnés;

2) de fournir des informations clientèle à des tiers sur demande écrite du client et

3) de fournir des informations clientèle sous forme agrégée.

[47 USC, § 222 c) 1)-3).] La loi autorise également une exception dans l'utilisation des informations relatives à la clientèle de la part des entreprises de télécommunications:

1) pour la mise en service, la prestation, la facturation et l'encaissement de leurs services;

2) pour la protection contre les comportements frauduleux, abusifs ou illicites et

3) pour fournir des services de télémarketing, d'assistance ou administratifs durant un appel lancé par le client [2].

[*Idem*, § 222 d) 1)-3).] Enfin, les entreprises de télécommunications sont tenues de fournir aux éditeurs d'annuaires téléphoniques des informations sur la liste de leurs abonnés, qui ne peuvent comporter que les noms, adresses, numéros de téléphone et professions dans le cas des clients commerciaux [*idem*, § 222 e)].

L'exception pour «autorisations explicites» pourrait jouer lorsque les entreprises de télécommunications utilisent CPNI pour prévenir la fraude ou un autre comportement illicite. Même dans ce cas, de telles actions pourraient être considérées «d'intérêt public» et autorisées par les principes pour cette raison.

Réglementation proposée par le ministère de la santé

Le Department of Health and Human Services (HHS) a proposé des réglementations concernant la confidentialité des informations sanitaires identifiables de façon individuelle [voir 64 Fed. Reg. 59,918 (Nov. 3, 1999) (à codifier dans 45 CFR, points 160-164)]. Ces règles consisteraient dans l'application des dispositions relatives à la confidentialité du Health Insurance Portability and Accountability Act de 1997, Pub. L. 104-191. Les règles proposées interdiraient normalement aux organismes couverts (plans sanitaires, centres de documentation sanitaire et prestataires de soins sanitaires transmettant l'information sanitaire sous forme électronique) d'utiliser ou de divulguer des informations sanitaires sans autorisation des particuliers (voir proposition 45 CFR, alinéa 164.506). Les règles proposées n'autoriseraient la divulgation d'informations sanitaires protégées que pour deux motifs 1) permettre aux individus d'examiner et de copier des informations sanitaires les concernant (*idem*, alinéa 164.514) et 2) faire respecter les règles (*idem*, alinéa 164.522).

Les règles proposées permettraient l'utilisation ou la divulgation d'informations sanitaires protégées, sans autorisation spécifique, dans un nombre limité de circonstances. Celles-ci comprennent, par exemple, la supervision du système de

(1) De la même façon, le médecin de cet exemple ne pourrait s'en remettre à une autorisation légale pour s'affranchir de l'option qu'offre FAQ 12 aux individus de se retirer du *marketing* direct. Le champ de toute exception pour «autorisations explicites» est nécessairement restreint au champ de l'autorisation suivant la législation pertinente.

(2) Le champ de cette exception est très limité. Statuairement, l'entreprise de télécommunications ne peut utiliser CPNI que durant un appel lancé par le client. D'autre part, nous avons été informés par la FCC de ce que l'entreprise de télécommunications ne peut utiliser CNPI pour commercialiser des services sortant du cadre de la demande du client. Enfin, étant donné que le client doit approuver l'utilisation de CPNI à cette fin, cette disposition ne constitue pas réellement une «exception».

▼B

santé, l'application de la loi et les urgences (*idem*, alinéa 164.506). Les règles proposées exposent en détail les limites de ces utilisations et divulgations. De plus, les utilisations et les divulgations autorisées d'informations sanitaires protégées seraient limitées à la quantité minimale nécessaire (*idem*, alinéa 164.506).

Les utilisations explicitement autorisées par le projet de règlement sont généralement conformes aux principes de la «sphère de sécurité» ou sont par ailleurs autorisées par une autre exception. Par exemple, l'application de la loi et l'administration judiciaire sont autorisées, de même que la recherche médicale. D'autres utilisations, telles que la supervision du système de santé, la fonction de santé publique et les systèmes d'information sanitaire nationaux sont d'intérêt public. Les divulgations et vue du traitement des contributions et exonérations sanitaires sont nécessaires pour garantir l'assistance sanitaire. Les utilisations en cas d'urgence, pour la consultation d'un parent proche concernant un traitement là où le consentement du patient «ne peut être pratiquement ou raisonnablement obtenu», ou pour déterminer l'identité ou la cause du décès du défunt, protègent les intérêts vitaux de la personne concernée et d'autrui. Les utilisations en vue de la gestion des militaires du service actif et d'autres catégories particulières de personnes facilitent l'exécution correcte de la mission militaire ou de situations critiques similaires; en tout état de cause, de telles utilisations auront un impact limité, voire nul, sur les consommateurs de façon générale.

Ne reste autorisée que l'utilisation d'informations à caractère personnel par les structures sanitaires pour produire des annuaires de patients. Si cette utilisation peut difficilement être qualifiée d'intérêt «vital», il n'en reste pas moins que les annuaires bénéficient aux patients ainsi qu'à leurs amis et relations. D'autre part, le champ de cette utilisation autoriséeest intrinsèquement limité. Par conséquent, le recours à l'exception aux principes pour les utilisations «explicitement autorisées» par la loi à cette fin présente un risque minimal pour la vie privée des patients.

Fair Credit Reporting Act

La Commission européenne a exprimé la préoccupation suivant laquelle l'exception des «autorisations explicites» «obligerait effectivement à déterminer le caractère adéquat» du Fair Credit Reporting Act (FCRA). Tel n'est pas le cas. En l'absence de la détermination spécifique du caractère adéquat du FCRA, les organisations américaines qui s'en remettraient sinon à une telle détermination devraient promettre d'adhérer à tous égards aux principes de la «sphère de sécurité». Cela signifie que lorsque les exigences du FCRA dépassent le niveau de protection représenté dans les principes, les organisations américaines ont seulement le devoir d'obéir au FCRA. À l'inverse, lorsque le FCRA pourrait s'avérer insuffisant, ces organisations devront mettre en conformité leurs pratiques d'information avec les principes. L'exception ne devrait pas modifier cette évaluation de base. Selon ses termes, l'exception s'applique uniquement lorsque la législation pertinente autorise explicitement une conduite qui ne serait pas conforme avec les principes de la «sphère de sécurité». L'exception ne serait pas appliquée là où les exigences du FCRA ne répondent pas aux principes de la «sphère de sécurité» ([1]).

En d'autres termes, par «exception» nous n'entendons pas que ce qui n'est pas obligatoire serait «explicitement autorisé». D'autre part, l'exception ne s'applique que lorsque ce qui est explicitement autorisé par la loi américaine entre en contradiction avec les dispositions des principes de la «sphère de sécurité». La loi pertinente doit répondre à ces deux éléments avant que ne soit autorisée la non-conformité à ces principes.

L'alinéa 604 du FCRA autorise, par exemple, explicitement les *consumer reporting agencies* à publier des rapports de consommation dans diverses situations énumérées (FCRA, alinéa 604). Ce faisant, l'alinéa 604 autorise les *credit reporting agencies* à agir en contradiction avec les principes de la «sphère de sécurité», ce qui aurait pour effet que les *credit reporting agencies* devraient recourir à l'exception (à moins, bien entendu, que ne s'applique une autre exception). Les *credit reporting agencies* doivent se plier aux arrêts du tribunal et aux citations du «grand jury», et l'utilisation des dossiers de crédit par les organes autorisés, les organismes sociaux et de soutien à l'enfance a une finalité publique, [*idem*, alinéa 604 a) 1), 3) D) et 4)]. Par conséquent, la *credit reporting agency* n'aurait pas à cette fin à recourir à l'exception de «l'autorisation explicite». Lorsqu'elle opère comnformément aux instructions écrites du consommateur la *consumer reporting agency* respecte intégralement les principes de la «sphère de sécurité» [*idem*, alinéa 604 a) 2)]. De la même façon, des dossiers de

([1]) La présente discussion ne revient pas à admettre que le FCRA n'assure pas une protection «adéquate». Toute évaluation du FCRA doit envisager la protection assurée par la loi dans son intégralité et ne pas se focaliser sur les exceptions comme nous le faisons ici.

▼B

consommation peuvent être obtenus à des fins d'emploi uniquement moyennant l'autorisation écrite du consommateur [*idem*, alinéa 604 a) 3) B) et b) 2) A) ii)] et pour des opérations de crédit ou d'assurances qui ne sont pas engagées par le consommateur, uniquement si celui-ci n'a pas marqué son désaccord à ces demandes [*idem*, alinéa 604 c) 1) B)]. d'autre part, le FCRA interdit au *credit reporting agency* de fournir des informations médicales à des fins d'emploi sans l'autorisation du consommateur [*idem*, alinéa 604 g)]. Ces utilisations sont conformes aux principes de notification et de choix. Les autres finalités autorisées par l'alinéa 604 concernent les opérations impliquant le consommateur, et seraient donc autorisées par les principes pour cette raison [*idem*, alinéa 604 a) 3) A) et F)].

La dernière utilisation «autorisée» par l'alinéa 604 concerne les marchés de crédit secondaires [*idem*, alinéa 604 a) 3) E)]. Il n'y a pas de conflit entre l'utilisation de dossiers de consommation à cette fin et les principes de la «sphère de sécurité» en tant que tels. Il est vrai que le FCRA n'exige pas des *credit reporting agencies*, par exemple, qu'elles notifient les consommateurs et leur demandent leur accord lorsqu'elles publient des rapports à cette fin. Cependant, nous rappelons que l'absence d'une exigence ne vaut pas «autorisation explicite» d'agir de façon autre que ce qui a été prescrit. De la même façon, l'alinéa 608 autorise les *credit reporting agencies* à fournir certaines informations à caractère personnel aux organismes gouvernementaux. Cette «autorisation» ne justifierait pas qu'une *credit reporting agency* ignore ses engagements d'adhérer aux principes de la «sphère de sécurité». Cela contrase avec nos autres exemples dans lesquels les exceptions aux principes de notification affirmative et de possibilité de choix sont invoquées pour autoriser explicitement l'utilisation des données à caractère personnel sans notification ni choix.

Conclusion

Quelques lignes-forces peuvent se dégager de ce panorama, si limité soit-il, d'actes législatifs:

— «l'autorisation explicite» permet généralement l'utilisation ou la divulgation d'informations à caractère personnel sans l'accord préalable de l'individu concerné; ainsi, l'exception serait limitée aux principes de notification et de choix,

— dans la plupart des cas, les exceptions autorisées par la loi sont formulées de façon restrictive de manière à s'appliquer dans des situations spécifiques à des fins bien déterminées. Par ailleurs, la loi interdit l'utilisation ou la divulgation non autorisée d'informations à caractère personnel ne rentrant pas dans ces limites,

— dans la plupart des cas, et reflétant leur caractère législatif, l'utilisation ou la divulgation autorisée servent un intérêt public,

— dans pratiquement tous les cas, les utilisations autorisées soit sont intégralement cohérentes avec les principes de la «sphère de sécurité», soit se rattachent à l'une des autres exceptions autorisées.

Em conclusion, l'exception pour «autorisations explicites» inscrite dans la loi sera, selon toute probabilité, par nature relativement limitée dans son champ d'application.

C. **Fusions et acquisitions**

Le groupe de travail de l'article 29 a exprimé sa préoccupation pour ce qui est des situations dans lesquelles une organisation adhérant aux principes de la «sphère de sécurité» fait l'objet d'un rachat ou d'une fusion par (avec) une entreprise qui n'a pas pris l'engagement de se conformer aux principes de la «sphère de sécurité». Cependant, le groupe de travail semble avoir supposé que l'entreprise survivante ne serait pas tenue de se conformer aux principes de la «sphère de sécurité» s'agissant des informations à caractère personnel détenues par la firme faisant l'objet d'une acquisition, mais tel n'est pas nécessairement le cas dans la législation américaine. La règle générale aux États-Unis pour ce qui est des fusions et acquisitions veut qu'une société acquérant le capital d'une autre entreprise assume généralement les obligations et responsabilités de la société acquise [voir 15 Flechter Cyclopedia of the Law of Private Corporations § 7117 (1990); voir également Model Bus. Corp. Act § 11.06 3) (1979)] («la société survivante endosse toutes les responsabilités des entreprises participant à la fusion»). En d'autres termes, l'entreprise survivante dans une fusion ou acquisition d'une organisation adhérant à la «sphère de sécurité» par cette méthode serait liée par les engagements de cette dernière en matière de «sphère de sécurité».

De surcroît, même si la fusion ou l'acquisition était effectuée moyennant le transfert d'actifs, les responsabilités de l'entreprise acquise pourraient lier la firme

▼B

acquérante dans certaines circonstances (15 Flechter, § 7122). Même lorsque les responsabilités n'ont pas survécu à la fusion, il faut toutefois noter qu'elles ne survivraient pas à une fusion dans laquelle les données ont été transférées d'Europe conformément à un contrat — la seule alternative praticable en dehors de la «sphère de sécurité» pour les transferts de données à destination des États-Unis. En outre, les documents de la «sphère de sécurité» tels que révisés exigent que toute organisation de la «sphère de sécurité» informe le département du commerce de toute acquisition, de manière à ne permettre la poursuite du transfert des données vers l'organisation qui succède uniquement si celle-ci adhère à la «sphère de sécurité» (voir FAQ 6). De fait, les États-Unis ont à présent révisé le cadre de la «sphère de sécurité» de manière à exiger des sociétés américaines se trouvant dans cette situation qu'elles effacent l'information qu'elles ont reçue dans le cadre de la «sphère de sécurité» si leurs engagements en matière de «sphère de sécurité» ne sont pas maintenus ou si des sauvegardes adéquates ne sont pas mises en place.

▼B

ANNEXE V

14 juillet 2000

John Mogg
Directeur, DG XV
Commission européenne
Bureau C 107-6/72
Rue de la Loi 200
B-1049 Bruxelles

Monsieur,

Il semblerait que la lettre que je vous ai adressée le 29 mars 2000 ait suscité une série de questions. Afin de préciser les attributions de la Commission fédérale du commerce (FTC) dans certains domaines, je vous transmets la présente qui, pour faciliter nos échanges futurs, complète et récapitule en partie la teneur de nos précédents courriers.

Dans le cadre de vos visites dans nos bureaux et de votre correspondance, vous avez soulevé plusieurs questions sur l'autorité de la Commission fédérale du commerce des États-Unis en matière de protection de la vie privée sur l'Internet. J'ai pensé qu'il serait utile de résumer mes précédentes réponses ainsi que de vous fournir de plus amples informations sur la compétence de la FTC concernant les problèmes de protection de la vie privée du consommateur que vous avez évoqués dans votre dernière lettre. Plus précisément, vous demandez: 1) si la FTC est compétente pour les transferts de données relatives à l'emploi effectués en violation des principes américains de la «sphère de sécurité», 2) si la FTC est compétente pour les systèmes d'agrément non lucratifs, 3) si le FTC Act s'applique aussi bien aux données en ligne qu'aux données hors ligne et 4) ce qui se passe lorsque les attributions de la FTC empiètent sur celles d'autres organes chargés de l'application de la loi.

Application du FTC Act à la protection de la vie privée

Dans ce domaine, la compétence de la Commission fédérale du commerce est définie à la section 5 du Federal Trade Commission Act («FTC Act»), qui interdit les manœuvres ou pratiques déloyales ou frauduleuses dans le commerce ([1]). Par «pratique frauduleuse», on entend une présentation, une omission ou une pratique susceptible d'induire réellement en erreur des consommateurs sensés. Une pratique est considérée comme déloyale si elle cause — ou est susceptible de causer — aux consommateurs un préjudice grave qui ne peut être raisonnablement évité et qui n'est pas compensé par des avantages pour les consommateurs ou la concurrence ([2]).

Certaines métohodes de collecte de données sont susceptibles d'enfreindre le FTC Act. Ainsi, si un site Internet prétend faussement observer une politique de protection de la vie privée ou une série de principes d'autoréglementation, la section 5 du FTC Act fournit une base juridique qui permet d'attaquer cette présentation erronée des faits comme étant frauduleuse. En effet, l'application réussie de la loi nous a permis d'établir ce principe ([3]). La FTC a, en outre, adopté le point de vue selon lequel elle peut contester les pratiques portant gravement atteinte à la protection de la vie privée lorsque celles-ci concernent des enfants ou l'utilisation d'informations de nature très sensible telles que les registres financiers ([4]) ou les dossiers médicaux. La Commission fédérale du commerce continuera de veiller à l'application de la loi en s'appuyant sur nos actions de suivi

([1]) 15 USC, § 45. Le Fair Credit Reporting Act s'appliquerait également à la collecte et à la vente de données Internet correspondant aux définitions légales de «rapport sur les consommateurs» et d'«agences d'étude de la consommation».

([2]) 15 USC, § 45 n).

([3]) Voir GeoCities, dossier nº C-3849 (jugement définitif du 12 février 1999) (www.ftc.gov/os/1999/9902/9823015d%26o.htm); Liberty Financial Cos., dossier nº C-3891 (jugement final du 12 août 1999) (www.ftc.gov/opa/1999/9905/younginvestor.htm). Voir également Children's Online Privacy Protection Act Rule (COPPA), 16 CFR, partie 312 (www.ftc.gov/opa/1999/9910/childfinal.htm). Le règlement COPPA, qui est entré en vigueur le mois dernier, prévoit que les opérateurs de sites Internet qui s'adressent à des enfants de moins de 13 ans ou qui collectent sciemment des données à caractère personnel auprès d'enfants de moins de 13 ans doivent appliquer les principes du code de déontologie de l'information énoncés dans le règlement.

([4]) Voir FTC v. Touch Tone, Inc., «Civil Action nº 99-WM-783» (D. Co.) (enregistrée le 21 avril 1999) («www.ftc.gov/opa/1999/9904/touchtone.htm». Avis du personnel du 17 juillet 19978, en réponse à une pétition déposée par le Center for Media Education («www.ftc.gov/os/1997/9707/cenmed.htm».

▼B

et de recherche ainsi que sur les cas soumis par des organisations d'autoréglementation et autres, y compris les États membres de l'Union européenne.

Contribution à l'autoréglementation

La FTC accordera la priorité aux cas de non-respect des principes d'autoréglementation soumis par des organisations telles que BBBOnline ou TRUSTe [1]. Cette approche est cohérente avec les relations que nous entretenons de longue date avec le National Advertising Review Board (NARB) du Better Business Bureau, qui porte les réclamations en matière de publicité devant la FTC. La National Advertising Division (NAD) du NARB traite les plaintes en matière de publicité au niveau national par voie d'arbitrage. Lorsqu'une partie refuse de se conformer à une décision de la NAD, l'affaire est renvoyée devant la FTC. Le personnel de la FTC examine, en priorité, la publicité contestée afin de déterminer si elle enfreint le FTC ACt. Elle réussit fréquemment à mettre un terme à la pratique incriminée ou à convaincre la partie intéressée de respecter le processus du NARB.

De même, la FTC se penchera en priorité sur les cas de non-respect des principes de la «sphère de sécurité» présentés par des États membres de l'Union européenne. À l'instar des demandes émanant des organisations d'autoréglementation américaines, nos collaborateurs tiendront compte de toutes les informations permettant de déterminer si la pratique contestée enfreint la section 5 du FTC Act. Cet engagement est également exprimé dans les principes de la «sphère de sécurité» (question souvent posée, FAQ 11, relative à l'application des décisions).

GeoCities: le premier cas de non-respect de la protection de la vie privée sur l'Internet traité par la FTC

GeoCities, le premier cas de non-respect de la protection de la vie privée sur l'Internet a été traité par la Commission fédérale du commerce en vertu de la section 5 [2]. Dans cette affaire, la FTC a fait valoir que GeoCities présentait de manière trompeuse, aussi bien aux enfants qu'aux adultes, la manière dont il entendait utiliser les données à caractère personnel les concernant. Selon l'action engagée, GeoCities aurait indiqué que certaines données à caractère personnel recueillies sur son site Internet n'étaient destinées qu'à un usage interne ou pour fournir aux consommateurs des offres promotionnelles, des produits ou des services répondant à leurs demandes et que des données supplémentaires «facultatives» ne seraient pas divulguées sans le consentement du consommateur. Or, ces informations ont été communiquées à des tiers qui les ont utilisées afin de solliciter les consommateurs au-delà des limites qu'ils avaient acceptées. GeoCities est également accusé de recourir à des pratiques frauduleuses en matière de collecte d'informations auprès des enfants. GeoCities prétendait gérer des pages réservées aux enfants sur son site Internet et conserver les informations recueillies dans ce cadre. Or, ces pages étaient en fait gérées par des tiers qui ont collecté et gardé les données.

Le règlement du litige interdit à GeoCities de déformer les fins auxquelles il collecte ou utilise des informations à caractère personnel concernant les

(1) En effet, la FTC a récemment porté plainte devant une cour de district fédéral contre un détenteur du sceau TRUSTe, Toysmart.com, demandant à ce titre que des mesures contraignantes et déclaratoires soient prises afin d'empêcher la vente d'informations nominatives (sur la clientèle) que cette société collectait sur son site Internet en violation de ses propres principes de protection de la vie privée. La FTC a été informée directement par TRUSTe de cette infraction présumée. FTC v. Toysmart.com, LLC, «Civil Action nº 00-11341-RGS (D.Ma.)», enregistrée le 11 juillet 2000 (www.ftc.gov/opa/2000/07/toysmart.htm).

(2) GeoCities, dossier nº C-3849 (jugement définitif du 12 février 1999) (www.ftc.gov/os/1999/9902/9823015d%26o.htm).

▼B

consommateurs, y compris les enfants. Aux termes du jugement, la société est tenue de placer sur son site Internet une note claire et visible sur la protection de la vie privée, qui indique aux consommateurs quelles sont les données recueillies et à quelle fin, à qui elles seront communiquées et comment ils peuvent accéder à ces données et les supprimer. Afin de garantir un contrôle parental, GeoCities doit obtenir l'accord des parents avant de collecter des informations à caractère personnel auprès des enfants de moins de 13 ans. GeoCities est tenu d'informer ses membres et de leur donner la possibilité de faire rayer les informations les concernant des bases de données de GeoCities et de tiers. Le règlement prévoit expressément que GeoCities doit informer les parents des enfants de moins de 13 ans et effacer les informations correspondantes, à moins que les parents ne consentent à ce que ces données soient conservées et utilisées. Enfin, GeoCities doit demander aux tiers qui il a précédemment communiqué des informations de les effacer ([1]).

ReverseAuction.com

En janvier 2000, la FTC a déclaré recevable la plainte déposée contre ReverseAuction.com et adopté une convention d'expédient avec cette société. Ce site de vente aux enchères en ligne aurait obtenu des informations à caractère personnel sur des consommateurs d'un site concurrent (eBay.com), puis envoyé des messages électroniques frauduleux et non sollicités aux consommateurs intéressés par leurs activités ([2]). Nous avons fait valoir que ReverseAuction avait enfreint la section 5 du FTC Act en obtenant des données à caractère personnel, comprenant les adresses électroniques et les codes d'identification personnels des utilisateurs, d'eBay, de même qu'en envoyant des messages électroniques frauduleux.

Comme le décrit la plainte, avant d'obtenir ces informations, ReverseAuction s'est abonné à eBay et a souscrit à l'accord pour la protection de la vie privée des utilisateurs de cette société. Cet accord protège la vie privée des consommateurs en interdisant aux utilisateurs d'eBay de recueillir et d'utiliser des données à caractère personnel à des fins non autorisées, telles que l'envoi de messages électroniques commerciaux non sollicités. Par conséquent, nous avons, tout d'abord, fait valoir que ReverseAuction a menti en déclarant qu'il respecterait l'accord pour la protection de la vie privée des utilisateurs d'eBay, ce qui constitue une pratique frauduleuse au titre de la section 5. Nous avons, en outre, prétendu que l'utilisation, par ReverseAuction, de ces informations en vue d'envoyer des messages électroniques commerciaux non sollicités, en violation de l'accord pour la protection de la vie privée des utilisateurs, constituait une pratique commerciale déloyale aux termes de la section 5.

Ensuite, nous avons signalé que les messages électroniques envoyés aux consommateurs contenaient une ligne «objet» susceptible de les induire en erreur puisqu'elle informait chacun d'entre eux que leur code d'identification eBay «allait bientôt expirer». Enfin, nous avons allégué que les messages électroniques laissaient entendre, à tort, qu'eBay fournissait à ReverseAuction, directement ou indirectement, des données à caractère personnel sur ses utilisateurs ou participait à la diffusion de messages électroniques non sollicités.

Le règlement du litige obtenu par la FTC interdit à ReverseAuction de commettre de pareilles infractions à l'avenir. Il fait également obligation à ReverseAuction de fournir une note d'information aux consommateurs qui se sont inscrits ou qui souhaitent s'inscrire sur ReverseAuction après avoir reçu un e-mail de ce site. La note informe ces consommateurs que leur «user ID» auprès d'eBay n'était pas sur le point d'expirer et qu'eBay n'avait pas été informé de la diffusion du courrier électronique non sollicité par ReverseAuction et n'avait pas autorisé cette

([1]) Par la suite, la FTC a résolu une autre affaire concernant la collecte sur l'Internet de données à caractère personnel auprès d'enfants. Liberty Financial Companies Inc., gérait le site Internet Young Investor qui s'adressait aux enfants et aux adolescents et était axé sur les questions d'argent et d'investissement. La FTC a fait valoir que le site indiquait faussement que les données à caractère personnel recueillies auprès des enfants à l'aide d'une enquête seraient conservées de manière anonyme et que les participants recevraient un bulletin d'information électronique ainsi que des lots. En réalité, les données personnelles concernant les enfants et la situation financière de la famille étaient conservées de manière identifiable et aucun bulletin ni lot n'ont été envoyés. La convention d'expédient interdit ces présentations erronées à l'avenir et impose à Liberty Financial de placer une note d'information sur la protection de la vie privée sur ses sites pour enfants ainsi que d'obtenir le consentement vérifiable des parents avant de collecter des données à caractère personnel auprès des enfants. Liberty Financial Cos., dossier nº C-3891 (jugement définitif du 12 août 1999) (www.ftc.gov/opa/1999/9905/younginvestor.htm).

([2]) Voir ReverseAuction.com, Inc.,«Civil Action nº 000032» (DDC) (enregistrée le 6 janvier 2000) (le communiqué de presse et les actes de procédure peuvent êtte consultés à l'adresse suivante: www.ftc.gov/opa/2000/01/reverse4.htm).

▼B

opération. La note donne également l'occasion à ces consommateurs d'annuler leur inscription auprès de ReverseAuction et de faire supprimer les informations à caractère personnel de la base de données de ce site. En outre, le jugement rendu fait obligation à ReverseAuction d'effacer les informations à caractère personnel concernant les abonnés d'eBay qui ont reçu le courrier de ReverseAuction sans être inscrits sur ce site et interdit l'utilisation ou la divulgation de telles données. Enfin, conformément aux décisions antérieures obtenues par la FTC en matière de protection de la vie privée, le jugement commande à ReverseAuction de diffuser ses principes de protection de la vie privée sur son site Internet et contient des dispositions exhaustives en matière d'enregistrement des données qui permettent à la FTC de surveiller la mise en œuvre de ces principes.

L'affaire ReverseAuction montre que la FTC est déterminée à prendre des mesures d'exécution pour renforcer les codes d'autoréglementation appliqués par les entreprises en ce qui concerne la protection de la vie privée des consommateurs sur l'Internet. Le règlement de cette affaire a en effet permis de mettre un terme à des pratiques contraires à un accord pour la protection de la vie privée et susceptibles d'entamer la confiance des consommateurs dans les mesures de protection prises par les sociétés de vente sur l'Internet. Étant donné que cette affaire concernait des informations à caractère personnel détournées par une entreprise, alors qu'elles étaient protégées par des principes établis par une autre entreprise, elle peut également revêtir un certain intérêt dans le cadre des problèmes de protection de la vie privée soulevés par le transfert de données entre entreprises de différents pays.

Même si la Commission fédérale du commerce a engagé des actions coercitives dans les cas de GeoCities, Liberty Financial Cos. et ReverseAuction, elle a une compétence plus limitée dans certains domaines de la protection de la vie privée sur l'Internet. Comme cela a été indiqué plus haut, les informations à caractère personnel collectées et utilisées sans l'accord des personnes concernées ne sont soumises aux dispositions de la loi sur la FTC que si elles s'inscrivent dans le contexte de pratiques commerciales déloyales ou frauduleuses. Par conséquent, la loi sur la FTC ne s'applique sans doute pas aux pratiques d'un site web qui collecte des informations à caractère personnel auprès des consommateurs sans pour autant cacher l'objectif de cette opération ou utiliser/diffuser ces données à des fins susceptibles de porter gravement préjudice aux consommateurs. En outre, la FTC n'est actuellement pas en mesure d'exiger systématiquement des entités qui collectent des informations sur l'Internet d'adhérer à un mécanisme de protection de la vie privée ou de souscrire à l'un de ces mécanismes en particulier ([1]). Toutefois, comme cela a été indiqué ci-dessus, une entreprise qui ne respecte pas ses engagements en matière de protection de la vie privée est susceptible de commettre par la même un acte frauduleux.

En outre, le domaine de compétence de la FTC n'englobe les manœuvres et les pratiques déloyales ou frauduleuses que si celles-ci sont de nature «commercia-

([1]) C'est pourquoi la Commission fédérale du commerce a déclaré, dans le cadre d'une audition devant le Congrès, que des textes législatifs supplémentaires seraient sans doute nécessaires pour obliger l'ensemble des sites Internet américains à vocation commerciale à adopter des pratiques précises en ce qui concerne l'information objective des consommateurs (voir «Consumer Privacy on the World Wide Web», témoignage présenté le 21 juillet 1998 au sous-comité des télécommunications, du commerce et de la protection des consommateurs du comité du commerce de la Chambre des représentants des États-Unis; ce document peut être consulté à l'adresse suivante: (www.ftc.gov/os/9807/privac98.htm). La FTC n'a pas encore sollicité l'élaboration d'une telle législation afin que les entreprises optant pour des codes d'autoréglementation puissent démontrer que les bonnes pratiques en matière d'information sur les sites web sont largement diffusées. Dans le rapport sur la protection de la vie privée sur l'Internet présenté au Congrès en juin 1998 («Privacy Online: A Report to Congress»); ce document peut être consulté à l'adresse suivante: (www.ftc.gov/reports/privacy3/toc.htm), la FTC a recommandé l'adoption de textes législatifs obligeant les sites web commerciaux à obtenir un accord parental avant de collecter des informations à caractère personnel auprès d'enfants de moins de 13 ans (voir note 3 de bas de page ci-dessus). L'année dernière, la FTC a constaté, dans son rapport intitulé «Self-Regulation and Privacy Online: A Federal Trade Commission Report to Congress» (juillet 1999, ce document peut être consulté à l'adresse suivante: www.ftc.gov/os/1999/9907/index.htm#13), que des progrès satisfaisants avaient été obentus en matière d'autoréglementation; en conséquence, elle a décidé à cette époque de ne pas recommander l'élaboration de textes de loi.
En mai 2000, la Commission a soumis un troisième rapport au Congrès: «Privacy Online: Fair Information Practices in the Electronic Marketplace» (www.ftc.gov/os/2000/05/index.htm#22). Ce document analyse l'enquête récemment menée par la FTC en ce qui concerne les sites Internet commerciaux et leur respect des pratiques équitables en matière d'information. Il contient, en outre, une recommandation (votée par la majorité de la FTC) qui invite le Congrès à passer une législation définissant un niveau élémentaire de protection de la vie privée pour les sites Internet commerciaux s'adressant aux consommateurs.

▼B

les». Les informations collectées par des entités commerciales qui font la promotion de produits ou de services, y compris les informations collectées et utilisées à des fins commerciales, entrent probablement dans le domaine de compétence de la FTC. En revanche, un grand nombre de particuliers et d'entités collectent des informations sur l'Internet sans poursuivre d'objectif commercial, de sorte qu'ils ne relèvent pas de la FTC. On peut citer, à titre d'exemple, les «forums de discussion» gérés par des entités non commerciales, notamment par des organismes d'utilité publique.

Il convient, enfin, de noter que le domaine de compétence fondamental de la FTC en matière de pratiques commerciales est soumis à un certain nombre d'exclusions légales totales ou partielles, ce qui limite la capacité de la FTC à fournir une réponse exhaustive aux problèmes de protection de la vie privée sur l'Internet. Ces exclusions concernent un grand nombre d'entreprises ayant largement recours aux informations sur les consommateurs, telles que les banques, les sociétés d'assurance et les compagnies aériennes. Comme vous le savez, ces entités relèvent de la compétence d'autres agences au niveau fédéral ou au niveau des États, notamment les agences fédérales chargées des questions bancaires et le ministère des transports.

Dans les affaires qui la concernent, la FTC enregistre les plaintes déposées par les consommateurs [par courrier électronique, par téléphone et — depuis peu — sur son site web (1)] auprès de son centre de réponse aux consommateurs (CRC). Le CRC enregistre toutes les plaintes déposées par les consommateurs, y compris ceux qui résident dans les États membres de l'Union européenne. La loi relative à la FTC permet à la Commission fédérale du commerce d'obtenir des mesures de redressement par voie d'injonction contre toute infraction à ladite loi ainsi que la réparation des préjudices subis par les consommateurs. En cas de plainte, nous nous efforçons toutefois de vérifier si l'entreprise mise en cause s'est livrée, de façon répétée, à des pratiques abusives, car nous ne traitons par les contentieux individuels dans le domaine de la consommation. Par le passé, la Commission fédérale du commerce a obtenu des réparations pour des citoyens des États-Unis et d'autres pays (2). La FTC continuera, le cas échéant, à imposer son autorité afin d'obtenir des réparations pour les citoyens d'autres pays ayant subi un préjudice par suite de pratiques frauduleuses relevant de la compétence de la FTC.

Données sur l'emploi

Dans votre dernière lettre, vous avez demandé des précisions supplémentaires sur les attributions de la FTC dans le domaine des données sur l'emploi. Vous demandez tout d'abord si la FTC peut prendre des mesures en vertu de la section 5 contre une entreprise qui affirme mettre en œuvre les principes de la «sphère de sécurité», mais qui transfère ou utilise des données sur l'emploi de façon contraire à ces principes. Nous souhaitons vous assurer que nous avons soigneusement examiné les dispositions législatives qui définissent le mandat de la FTC, de même que les documents connexes et la jurisprudence, et que nous avons conclu que la FTC a la même compétence pour les données liées à l'emploi que pour toute autre donnée relevant de la section 5 du FTC Act (3). En d'autres termes, nous pouvons prendre des mesures dans le cas des données liées à l'emploi si une affaire de protection de la vie privée répond aux critères qui nous imposent la prise de mesures d'exécution (pratiques déloyales et frauduleuses).

Nous souhaitons également dissiper les doutes qui existeraient quant à la capacité de la FTC de ne prendre des mesures d'exécution que dans les cas où une entreprise porte préjudice à des consommateurs particuliers. En fait, comme l'action de la FTC dans l'affaire ReverseAuction (4) le montre clairement, la FTC engage une procédure de mise en œuvre dans les affaires concernant la protection

(1) Voir https://www.ftc.gov/ftc/complaint.htm pour consulter le formulaire de dépôt de plainte sur le site de la Commission fédérale du commerce.

(2) Ainsi, dans une récente affaire de pyramide financière sur l'Internet, la FTC a obtenu des remboursements d'un montant total d'environ 5,5 millions de dollars pour 15 622 consommateurs. Ceux-ci résidaient aux États-Unis et dans soixante-dix pays étrangers (voir www.ftc.gov/opa/9807/fortunar.htm; www.ftc.gov/opa/9807/ftcrefund01.htm).

(3) Il convient, cependant, de noter une exception (qui est expressément signalée dans les dispositions législatives définissant le mandat de la FTC): les compétences que la loi sur la FTC confère à cette Commission dans le domaine des pratiques «commerciales» coexistent avec les pouvoirs constitutionnels du congrès aux termes de la clause sur le commerce [United States v. American Building Maintenance Industries, 422 US 271, 277 n. 6 (1975)]. Le domaine de compétence de la FTC englobe donc les pratiques mises en œuvre en matière d'emploi par les entreprises et les branches du commerce international.

(4) «Online Auction Site Settles FTC Privacy Charges», communiqué de presse de la FTC (6 janvier 2000), disponible à l'adresse suivante: http://www.ftc.gov/opa/2000/01/reverse4.htm.

▼B

de la vie privée lorsque, dans le cadre de transfert de données entre entreprises, l'une des entreprises concernées commet une infraction vis-à-vis de l'autre entreprise, portant éventuellement préjudice aux consommateurs et aux entreprises elles-mêmes. Nous pensons qu'il s'agit là du cas de figure dans lequel la question des données sur l'emploi est la plus susceptible de se poser, car les données de ce type concernant des citoyens européens sont transférées par des entreprises européennes à des entreprises américaines qui ont pris l'engagement de respecter les principes de la «sphère de sécurité».

Nous tenons toutefois à signaler que, dans certaines circonstances, la marge de manœuvre de la FTC est limitée, notamment lorsqu'une affaire est déjà traitée dans le cadre d'un litige traditionnel de droit du travail (le plus probable étant une réclammation ou une demande d'arbitrage ou encore une plainte déposée auprès du National Labor Relations Board pour pratiques frauduleuses dans le domaine du droit du travail). Tel serait le cas, par exemple, si un employeur avaitpris un engagement concernant l'utilisation de données à caractère personnel dans le cadre d'un accord collectif et qu'un salarié ou un syndicat affirmait que cet employeur ne respecte pas ledit accord. La FTC n'interviendrait probablement pas dans une telle procédure (1).

Compétence en matière de systèmes «d'agrément» (seal programs)

Vous demandez ensuite si la FTC est compétente en ce qui concerne les systèmes «d'agrément» permettant de gérer des mécanismes de résolution des litiges aux États-Unis, lorsque ces systèmes abusent de leur fonction en assurant la mise en œuvre des principes de la «sphère de sécurité» et en traitant les plaintes individuelles, alors que — techniquement — ces systèmes sont des organismes à but non lucratif. Pour déterminer si une entité qui déclare être sans but lucratif relève de la compétence de la FTC, nous étudions soigneusement si cette entité, à supposer qu'elle ne cherche pas à faire des bénéfices pour son propre compte, favorise l'enrichissement de ses membres. La Commission a fait valoir avec succès qu'elle était compétente dans ce domaine et la Cour suprême des États-Unis a d'ailleurs déclaré à l'unanimité, le 24 mai 1999, que la FTC avait juridiction sur une association privée à but non lucratif regroupant des groupes locaux de dentistes dans une affaire antitrust (California Dental Association v. Federal Trade Commission). La Cour a estimé que:

«La loi sur la FTC doit porter non seulement sur les entités qui cherchent à faire des bénéfices pour leur propre compte (15 USC, § 44), mais aussi sur les entités qui visent à obtenir des profits pour le compte de leurs membres. [...] Il paraît en effet difficile de croire que le Congrès a souhaité l'adoption d'une notion aussi étroite des organisations d'aide, étant donné qu'une telle restriction permettrait à certaines organisations de ne pas être soumises à la FTC dans les affaires exigeant l'intervention de celle-ci.»

En somme, pour déterminer si elle a juridiction sur une entité particulière «à but non lucratif» gérant un système d'agrément, la Commission fédérale du commerce doit examiner concrètement dans quelle mesure une telle entité permet à ses membres de faire des bénéfices. Si ladite entité gère son système d'agrément de façon à obtenir des profits pour ses membres, il est probable que la FTC se déclare compétente. Par ailleurs, la FTC aurait probablement juridiction sur les systèmes frauduleux se faisant passer pour des entités à but non lucratif.

Protection des données «hors ligne» à caractère personnel

De plus, vous notez que notre correspondance antérieure avait essentiellement été axée sur la protection de la vie privée dans le cadre des activités en ligne. Si ce domaine est l'une des préoccupations majeures de la FTC, étant donné qu'il constitue l'un des principaux éléments du développement du commerce électronique, il reste que la loi sur la FTC date de 1914 et s'applique également aux activités hors ligne. Par conséquent, nous sommes habilités à poursuivre les entreprises qui adoptent des pratiques commerciales déloyales ou frauduleuses en matière de protection de la vie privée des consommateurs (2). En fait, dans une

(1) La question de savoir si une pratique est contraire au droit du travail ou à un accord collectif est un problème technique relevant habituellement des tribunaux spécialisés, notamment les instances d'arbitrage et le National Labor Relations Board (NLRB).

(2) Comme vous le savez, le Fair Credit Reporting Act donne également à la FTC le pouvoir de protéger la confidentialité des données personnelles à caractère financier dans le cadre du champ d'application de la loi et la FTC a récemment pris une décision ayant trait à ce problème («In the Matter of Trans Union», dossier nº 9255, 1er mars 2000, communiqué de presse et avis disponibles à l'adresse suivante: www.ftc.gov/os/2000/03/index.htm#1).

▼B

affaire soumise l'année dernière à la FTC [FTC v. TouchTone Information Inc. (1), un «négociant en informations» a été chargé d'obtenir et de vendre illégalement des données confidentielles sur la situation financière de certains consommateurs. La FTC a fait valoir que TouchTone avait obtenu ces informations sous de faux prétextes, en utilisant des techniques d'investigation employées à l'origine par des enquêteurs privés pour obtenir des renseignements à caractère personnel, généralement par téléphone. Dans cette affaire, enregistrée le 21 avril 1999 devant une cour fédérale dans le Colorado, le procureur demande une injonction et le remboursement de l'ensemble des bénéfices obtenus illégalement.

Cette expérience de l'application des lois, de même que l'intérêt récemment porté à la fusion de bases de données en ligne et hors ligne, à la limite de plus en plus floue entre les opérateurs en ligne et hors ligne, et au fait qu'un volume considérable d'informations nominatives est collecté et utilisé hors ligne, fait clairement apparaître la nécessité d'être particulièrement attentif à la protection de la vie privée hors ligne.

Chevauchement de compétences

Enfin, vous posez la question du chevauchement de compétences entre la FTC et les autres agences concernées. Nous avons noué des liens de travail étroits avec de nombreuses autres agences, y compris avec des agences fédérales surveillantles activités bancaires et les procureurs généraux des États. Nous coordonnons souvent les enquêtes afin d'exploiter au mieux nos ressources en cas de chevauchement de compétences. En outre, nous soumettons souvent des problèmes pour enquête aux agences fédérales ou aux agences des États.

J'espère que cet aperçu vous sera utile et je reste à votre disposition pour tout renseignement supplémentaire.

[Formule de politesse]

Robert Pitofsky

(1) «Civil Action 99-WM-783 (D Colo.)», disponible à l'adresse suivante: http://www.ftc.gov/opa/1999/9904/touchtone.htm (dans l'attente d'un jugement d'accord provisoire).

▼B

ANNEXE VI

John Mogg
Directeur général de la DG XV
Commission européenne
Bureau C 107-6/72
Rue de la Loi 200
B-1049 Bruxelles

Monsieur le Directeur général,

Je vous adresse le présent courrier à la demande du ministère américain du commerce afin de vous expliquer le rôle du ministère des transports dans la protection de la vie privée des consommateurs concernant les informations fournies par ceux-ci aux compagnies aériennes.

Le ministère des transports est favorable à l'autoréglementation la moins contraignante et aux dispositifs les plus efficaces en vue de garantir le caractère privé des informations communiquées par les consommateurs aux compagnies aériennes. Par conséquent, il approuve la mise en place d'une «sphère de sécurité» permettant aux compagnies aériennes de se conformer aux dispositions de la directive européenne relative à la protection des données à caractère personnel transférées hors de l'Union européenne. Le ministère reconnaît toutefois que ces mesures ne peuvent être efficaces que si les compagnies aériennes tiennent réellement leur engagement à respecter les principes de protection de la vie privée prévus par la «sphère de sécurité». À cet égard, l'autoréglementation devrait être étayée par des mesures répressives. Le ministère fera donc appel à son autorité de surveillance de protection des consommateurs et garantira que les compagnies aériennes respectent les engagements en matière de protection de la vie privée pris vis-à-vis du public. Il instruira les plaintes pour non-respect présumé des engagements pris qui nous sont transmises par des organisations d'autoréglementation et autres, y compris les États membres de l'Union européenne.

Le ministère est habilité à prendre des mesures de mise en œuvre dans ce domaine en vertu du titre 49, section 41712, de l'USC, qui interdit à un transport «toute pratique arbitraire ou frauduleuse ou tout acte de concurrence déloyale» pour la vente de prestations de transport aérien qui porte ou risque de proter préjudice au consommateur. La section 41712 est calquée sur la section 5 de la loi sur la commission fédérale du commerce (15 USC 45). Cependant, les transporteurs aériens sont exemptés des dispositions de la section 5 de la loi par la commission fédérale du commerce en vertu du titre 15, section 45 a) 2), de l'USC.

Mes services examinent des affaires et engagent des poursuites dans certains cas en vertu du titre 49, section 41712, de l'USC (voir, par exemple, les ordonnances suivantes: 99-11-5 du ministère américain des transports du 9 novembre 1999; 99-8-23 du 26 août 1999; 99-6-1 du 1er juin 1999; 98-6-24 du 22 juin 1998; 98-6-21 du 19 juin 1998; 98-5-31 du 22 mai 1998 et 97-12-23 du 18 décembre 1997). Nous instruisons ce genre d'affaires sur la base de nos propres enquêtes et de plaintes officielles ou informelles déposées par des particuliers, des agences de voyages, des compagnies aériennes et des organes administratifs américains ou étrangers.

J'aimerais attirer votre attention sur le fait que le non-respect par un transporteur du caractère privé des informations communiquées par un passager ne constituerait pas une violation *a priori* de la section 41712. Toutefois, dès lors qu'un transporteur s'est formellement et publiquement engagé à observer les principes de la «sphère de sécurité» garantissant le respect du caractère privé des informations que lui a fournies le consommateur, le ministère peut faire usage des pouvoirs qui lui sont conférés par la section 41712 pour assurer le respect de ces principes. Par conséquent, lorsqu'un passager communique des informations à un transporteur qui s'est engagé à respecter les principes de la «sphère de sécurité», tout manquement à cet engagement serait susceptible de porter préjudice au consommateur et constituerait une violation de la section 41712. Mes services accordent la priorité à l'examen de tels cas et à des poursuites en cas de violation manifeste. Nous informons le ministère du commerce des résultats de ces actions.

Le non-respect des dispositions de la section 41712 peut entraîner l'émission d'ordonnances de ne pas faire et des sanctions de droit civil pour violation de ces ordonnances. Bien que nous n'ayons pas la compétence pour accorder des dommages-intérêts ou une réparation pécuniaire au plaignant, nous sommes habilités à sanctionner les règlements intervenant à la suite des enquêtes et des affaires examinées par le ministère qui prévoient l'octroi d'indemnités en nature aux consommateurs à titre de réparation ou pour compenser les amendements payables par ailleurs. Nous avons procédé ainsi par le passé et nous continuons et continuerons à le faire dans le cadre de la «sphère de sécurité» lorsque les

▼B

circonstances le justifient. Des infractions répétées à la section 41712 par une compagnie aérienne américaine mettraient également en doute la bonne volonté de celle-ci de respecter son engagement. Dans des situations extrêmes, on pourrait considérer qu'elle n'est plus apte à l'exploitation et, par conséquent, elle risquerait de perdre sa licence d'exploitation. [Voir ordonnances du ministère américain des transports 93-6-34 du 23 juin 1993 et 93-6-11 du 9 juin 1993.Bien que cette affaire ne portait pas sur la section 41712, elle a abouti à la révocation de la licence d'exploitation d'un transporteur pour violation complète des dispositions de la loi fédérale sur le transport aérien (Federal Aviation Act), d'un accord bilatéral et du règlement intérieur du ministère.]

J'espère que ces informations vous seront utiles. Je me tiens à votre disposition pour tout renseignement complémentaire.

Sincères salutations

Samuel Podberesky

Conseiller général adjoint
«Aviation Enforcement and Proceeding»

▼B

ANNEXE VII

Eu égard à l'article 1er, paragraphe 2, point b), les organes administratifs américains habilités à instruire les plaintes et à obtenir des mesures de redressement contre les pratiques déloyales ou frauduleuses ainsi que la réparation des préjudices subis par les personnes concernées, quel que soit leur pays de résidence ou leur nationalité, en cas de non-respect des principes mis en œuvre conformément aux FAQ sont:

1) la Commission fédérale du commerce et

2) le ministère du transport.

La Federal Trade Commission tire sa compétence de la section 5 du Federal Trade Commission Act. Ne relèvent pas de la compétence de la Federal Trade Commission au titre de la section 5: les banques, les entreprises financières d'épargne et de prêt et les coopératives de crédit, les sociétés de télécommunication et les entreprises publiques de transport inter-États, les transporteurs aériens, les chargeurs et les opérateurs d'entrepôt. Même si des compagnies d'assurances ne sont pas expressément citées dans la liste des exceptions figurant dans la section 5, la loi McCarran Fergusson [1] laisse la réglementation de l'assurance aux différents États. Toutefois, les dispositions du Federal Trade Commission Act s'appliquent au secteur de l'assurance dans la mesure où cette activité n'est pas réglementée par la loi de l'État. La Federal Trade Commission détient une compétence résiduelle pour les pratiques déloyales ou frauduleuses commises par les compagnies d'assurances dans le cadre d'activités qui ne relèvent pas du secteur de l'assurance.

Le ministère américain du transport vise la compétence au titre 49 du United States Code, section 41712. Le ministère américain du transport instruit les cas basés sur ses propres enquêtes ainsi que les plaintes formelles ou informelles reçues de particuliers, d'agents de voyage, de lignes aériennes, d'agences gouvernementales américaines ou étrangères.

[1] 5 USC, § 1011 et suivants.