2000

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Strasbourg, le 9 novembre 2000 T-PD-GR (2000) 2

**GROUPE DE REDACTION DU
COMITE CONSULTATIF DE LA CONVENTION POUR LA
PROTECTION DES PERSONNES A L'EGARD DU TRAITEMENT
AUTOMISE DES DONNEES A CARACTERE PERSONNEL (STE 108)**

5ème réunion
Strasbourg, 27-29 novembre 2000
Salle 3, Palais de l'Europe

ETUDE

RELATIVE AUX CONTRATS ENCADRANT LES TRANSFERTS DE DONNEES PERSONNELLES ENTRE LES PARTIES A LA CONVENTION 108 ET LES PAYS TIERS N'OFFRANT PAS UN NIVEAU DE PROTECTION ADEQUAT

Rapport de Jérôme Huet
Agrégé des facultés de droit
Professeur à l'Université de Paris II (Panthéon-Assas)
Directeur du CEJEM (Centre d'études juridiques et économiques du multimédia)

Document présenté par
la Direction Générale I (Affaires Juridiques)

SOMMAIRE

INTRODUCTION

Les pays européens disposent de législations protectrices des données personnelles faisant l'objet de traitements automatisés, en raison des dangers que ceux-ci font courir aux personnes concernées. Des législations ont été adoptées par ces pays à compter des années soixante-dix. Et le 28 janvier 1981, dans le cadre du Conseil de l'Europe, une convention a été signée portant sur la protection des personnes à l'égard du traitement automatisé de données à caractère personnelles, qui est entrée en vigueur en 1985.

L'existence de ces textes qui régissent les traitements de données dans les territoires nationaux sur lesquels ils sont applicables, a rendu nécessaire de réfléchir à la manière d'appréhender les transferts internationaux de ces données, transferts que l'existence des moyens de télécommunication numérisés permet aisément et que la mondialisation de l'économie rend inéluctables. La question, qui concerne au premier chef les rapports entre les entreprises privées de grande dimension, notamment celles ayant plusieurs implantations dans le Monde, présente un caractère particulièrement aigu si le transfert risque d'avoir lieu à destination d'un pays n'ayant pas un niveau de protection adéquat pour ces données.

L'article 12 de la convention de 1981, par exemple, prévoit qu'on puisse limiter ou interdire les flux transfrontières de données à destination d'Etats non contractants, et diverses législations nationales comportent des restrictions à ce sujet.

Intérêt des clauses contractuelles

Pour encadrer, et par là-même légitimer, ces échanges, on a eu l'idée de recourir à la technique contractuelle. De fait, il est apparu que des clauses organisant, dans les rapports entre une entreprise, "exportatrice" de données, et une autre entreprise, "importatrice" de ces données, les modalités de communication, d'utilisation et de conservation des données, seraient de nature à satisfaire aux exigences de la législation du pays de la première entreprise, si la seconde entreprise prenait des engagements permettant d'assurer la sécurité des informations en cause, le respect des finalités du traitement pour lequel elles ont été collectées, ainsi que les droits des personnes concernées.

Le postulat, à la base du système, est que, même dans des pays ne disposant pas de législation ou de mécanismes protecteurs des données personnelles, certaines entreprises, à la respectabilité indiscutable, peuvent prendre des engagements de nature à pallier l'absence de dispositif national, et à rendre juridiquement acceptable le transfert des informations en cause.

De telles clauses ont été mises au point par des instances internationales soucieuses de trouver une solution convenable pour ces transferts de données, Conseil de l'Europe, Chambre de commerce internationale, et par certaines autorités nationales en charge de la protection des données, dans le courant des années 90. Ainsi, le Conseil de l'Europe a-t-il pris l'initiative avec la Chambre de commerce internationale et la Communauté européenne de diffuser, en 1992, un "contrat type visant à assurer une protection équivalente des données dans le cadre des flux transfrontières de données" (doc. T-PD (92) 7 révisé).

Evolution de la problématique

L'évolution du droit depuis lors, notamment avec l'adoption par la Communauté européenne, en 1995, d'une directive 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, ainsi

que d'une directive propre au secteur des télécommunications en 1997, amène à procéder à l'évaluation de ce système.

La directive de 1995, au demeurant, comporte une disposition particulière concernant les transferts des données à destination de pays tiers, l'art. 25, aux termes duquel ceux-ci ne peuvent se faire que vers des pays qui leur assurent "un niveau de protection adéquat".

Un autre facteur de changement tient au développement des communications électroniques grâce à l'internet, et plus particulièrement à l'explosion du commerce électronique. De fait, le commerce électronique favorise la collecte de données personnelles, notamment sur les visiteurs de sites constitués par les entreprises, ou sur les clients. Les visiteurs et les clients sont d'ailleurs, souvent, sollicités lorsqu'ils reviennent sur un site, au moyen des "cookies" qui ont été implantés sur le disque dur de leur ordinateur lors de leur précédent passage. Les préoccupations pour la protection des personnes que suscitent ces pratiques, et d'autres encore, ont été débattues lors du sommet organisé par l'OCDE à Ottawa en 1998, et l'une des résolutions adoptées à cette occasion est "relative à la protection de la vie privée sur les réseaux mondiaux" (V. Rev. dr. informatiq. et télécoms, 1998-3, p. 101 s., le commentaire de E. Caprioli).

Cet aspect des choses, pour important qu'il soit, n'est, toutefois, pas au cœur du sujet traité. En effet, ce type d'application du commerce électronique met en jeu des rapports entre des entreprises et leurs clients ou prospects, et invite à s'interroger sur la manière dont les unes collectent des données sur les autres. Or, l'objet de l'étude est différent : celle-ci porte sur les transferts de données personnelles entre des entreprises, et sur les clauses contractuelles pouvant organiser ces transferts.

Définition du cadre de l'étude

Il a été demandé à l'auteur de la présente étude de procéder à une évaluation du mécanisme des clauses contractuelles utilisées pour le transfert de données personnelles, à la lumière des pratiques existantes et de l'évolution du contexte dans lequel elles s'opèrent.

Il a été demandé que cette évaluation soit faite avant tout au regard de la théorie générale des contrats. L'intérêt de l'étude est donc, principalement, de confronter les mécanismes mis en œuvre, dans ce domaine et pour ces objectifs particuliers, avec les règles qui gouvernent les obligations en général.

Accessoirement, l'étude aborde l'adéquation des modèles de clauses existants au regard de l'évolution de la protection des données durant les dernières années.

Observations liminaires

A ce stade, trois observations liminaires doivent être faites :

1° S'agissant de l'évolution de la protection des données personnelles, le texte pris en compte pour en témoigner est la directive de 1995 de la Communauté européenne, dont l'article 7 pose en principe qu'un traitement automatisé de telles données ne peut être effectué qu'avec le consentement de la personne concernée (consentement donné "indubitablement"),

et dont les art. 10 et 11 prévoient une information spécifique de la personne concernée lors de la collecte des données, ainsi que lors de leur communication à un tiers.

Accessoirement, sont pris en compte des textes comme l'accord CEE-USA du 20 juillet 2000 fondé sur les principes dits de la "sphère de sécurité" (ou encore "safe harbour principles").

2° En ce qui concerne les normes contractuelles, et en raison du fait que la problématique a nécessairement une dimension internationale, il n'était pas possible de se référer exclusivement à une législation nationale particulière : le choix a donc été fait de se fonder sur des principes universellement admissibles en la matière, comme sont les "Principes Unidroit pour les contrats commerciaux internationaux" (et V. sur le sujet, "Unidroit principles for international commercial contracts : a new lex mercatoria?", Chambre de commerce internationale, publication de l'Institut du droit et des pratiques du commerce international, 1995).

En tout état de cause, on présumera que les parties au transfert de données personnelles à destination d'un pays tiers à la Communauté européenne auront désigné, comme applicable à leur accord, la loi du pays d'établissement de l'exportateur, c'est-à-dire la loi d'un pays européen, et donc un droit qui est en harmonie avec les principes Unidroit. Dans l'accord CEE-USA du 20 juillet 2000, cependant, le droit déclaré applicable pour l'interprétation des principes de la "sphère de sécurité" est celui des Etats-Unis (accord précité).

3° Enfin, en ce qui concerne les pratiques existantes ont été examinés pour en tirer l'enseignement nécessaire à la définition de la problématique : le contrat-type élaboré conjointement par le Conseil de l'Europe, la CEE et la CCI en 1992 - et la version actuellement diffusée par la CCI -, ainsi que certains modèles d'accord proposés par des autorités nationales, notamment en Allemagne (Berlin), au Royaume-Uni (à destination du Commonwealth) et en Suisse; par ailleurs, les travaux initiés en 2000 par la Communauté européenne, dans le cadre de l'art. 26, §4, de la directive de 1995, ont également été pris en compte (V. l'avant projet de décision de la CEE sur les clauses-type pour le transfert des données à caractère personnel vers des pays tiers, septembre 2000).

Toutefois, il n'entrait pas dans le cadre de cette étude de faire un examen détaillé, éventuellement critique, des ces différents modèles contractuels. Ils ont seulement servi de base à la réflexion.

Afin de procéder à l'évaluation demandée, il est apparu nécessaire d'envisager le contrat de transfert de données dans les rapports entre les parties (I), puis de l'examiner au regard des rapports avec les tiers (II) avant, enfin, d'évoquer les modalités de règlement des litiges (III).

I. LE CONTRAT DE TRANSFERT DE DONNÉES ET LES RAPPORTS ENTRE LES PARTIES

Dans les rapports entre les parties, il convient, tout d'abord de caractériser l'objet du contrat et les obligations de chacune d'entre elles (A), puis d'évoquer les garanties de bonne exécution du contrat (B) et, enfin, les modalités de son dénouement (C).

A. L'OBJET DU CONTRAT ET LES OBLIGATIONS DES PARTIES

L'objet du contrat qui encadre le transfert de données personnelles peut être assez différent selon les situations (1°); mais les obligations des parties quant aux données transférées présentent toujours des points communs (2°).

1° L'objet du contrat

Plusieurs hypothèses peuvent se rencontrer. On peut distinguer trois catégories de situations particulièrement typiques.

- Premier cas : il s'agit de données concernant des clients et l'objectif poursuivi par l'exportateur de données est de les faire traiter dans un pays étranger, pour des raisons de coût ou pour concentrer dans ce pays les traitements de données du groupe auquel il appartient.

- Deuxième cas : les données concernent les salariés ainsi que les dirigeants des diverses entités d'un groupe de sociétés, implantées dans plusieurs pays, et leur transfert d'une entité à une autre est nécessaire au bon fonctionnement de l'ensemble du groupe.

- Troisième cas : il s'agit de données concernant des clients et des prospects d'une entreprise, qui les transfère à une autre entreprise située dans un pays étranger afin que celle-ci puisse les utiliser dans son activité commerciale de recherche de clientèle.

Quant aux données traitées elles peuvent être de nature très variées : celles concernant les clients peuvent être assez banales (nom, adresse, objet et montant des opérations...), mais elles seront parfois sensibles (exemple : dossier d'assurance-vie, informations relatives à la santé); celles concernant les salariés peuvent, elles aussi, ne pas être seulement triviales, mais concerner son intimité.

La diversité des cas de figure engendre des difficultés de qualification (a); on voit peu souvent, par ailleurs, les clauses contractuelles en usage distinguer selon les types de données personnelles transférées (b).

a) La qualification du contrat : dépôt ou cession

Le transfert de données personnelles peut être l'accessoire d'un contrat ou constituer son objet principal.

Lorsque les parties ont en vue, par exemple, le traitement de données personnelles par un sous-traitant (ainsi dans le cadre d'une opération d'externalisation, ou "outsourcing"), le contrat de prestation de service que constitue cette sous-traitance est l'objet principal du contrat. L'encadrement du transfert de données personnelles par un certain nombre d'obligations pesant sur les parties constitue l'accessoire de ce contrat principal.

En revanche, le transfert de données personnelles est l'objet principal du contrat dans des hypothèses comme celle où des données relatives à des clients ou prospects sont adressées par une entreprise à une autre, afin que cette dernière puisse s'en servir à des fins de prospection commerciale.

Dans la première hypothèse, on peut qualifier le transfert de données comme un dépôt accessoire à une prestation de service (un peu de la même manière qu'il y a dépôt lorsqu'on confie sa voiture pour réparation à un garagiste). La qualification de dépôt entre les mains

d'un tiers, en l'occurrence l'importateur de données, engendre un certain nombre de conséquences :

- l'exportateur de données conserve la maîtrise des données qui restent en son pouvoir de décision, car il les a seulement confiées à autrui;

- l'importateur de données ne saurait utiliser les données personnelles en cause pour ses besoins propres, ni *a fortiori* pour son propre profit;

- l'importateur de données doit les restituer (ou les détruire, s'agissant de biens immatériels susceptibles d'être reproduits) en fin de contrat;

- le contrat repose sur la confiance réciproque des parties et l'exportateur peut y mettre fin à tout moment si cette confiance est menacée.

Ainsi défini, ce type de situation peut être considéré comme présentant peu de risques pour les personnes concernées, et d'ailleurs l'avant projet de décision de la CEE sur les clauses-type pour le transfert des données à caractère personnel vers des pays tiers, de septembre 2000, semble la considérer comme tellement banale qu'elle l'exclut de son champ d'application (texte précité, art. 2, §2, *in fine* : "ce contrat ne concerne pas les transferts vers un sous-traitant tiers qui reste sous le contrôle de l'exportateur de données").

Dans la seconde hypothèse, l'opération de transfert de données est une cession d'information, et donc relève de la catégorie des contrats translatifs de propriété comme la vente. Tout dépend certes, juridiquement, du point de savoir si la loi applicable au contrat - on a souligné qu'il serait judicieux que les parties choisissent celle du pays de l'exportateur - admet qu'un fichier de clientèle constitue un bien immatériel protégé par une propriété intellectuelle (par exemple, la propriété littéraire et artistique). Mais, en tout état de cause, il est clair que les parties ont entendu laisser à l'importateur la possibilité d'exploiter les données dans le cadre de son activité professionnelle, au besoin en les combinant avec des informations provenant d'une autre source.

Cette qualification, à son tour, engendre un certain nombre de conséquences :

- l'exportateur perd largement la maîtrise des données en cause, dont il a concédé l'utilisation à un tiers;

- l'importateur a la faculté de se servir des données dans le cadre de son activité, et notamment d'en tirer un certain profit;

- en fin de contrat, il n'est pas nécessaire que les données soient restituées par l'importateur à l'exportateur;

- le contrat, ne reposant pas sur la confiance, ne peut pas être résilié unilatéralement.

La situation ainsi créée présente plus de risques, à l'évidence, pour les personnes concernées, à telle enseigne que le contrat-type du Conseil de l'Europe, de 1992, semble l'exclure lorsqu'il précise que "l'objectif n'est pas un transfert de propriété des données à caractère personnel, mais simplement un droit d'usage de ces données" (texte précité, point 33). Toujours est-il que l'hypothèse se rencontre fréquemment et que, d'ailleurs, le degré de danger doit être apprécié en fonction des types de donnés transférées : il peut être limité si les données ne sont pas sensibles.

De son côté, la Commission de la Communauté européenne semble bien avoir pris acte de cette possibilité, et des risques en découlant, puisque dans un des documents de travail sur le sujet elle déclare : "Il se peut que le destinataire du transfert ne fournisse pas simplement un service de traitement de données au responsable établi sur le territoire communautaire. En effet, il peut très bien avoir, par exemple, loué ou acheté les données pour les utiliser pour son propre compte et à ses propres fins. Le destinataire a alors besoin d'un certain degré de liberté pour traiter les données comme il l'entend et devient donc "responsable" du traitement à part entière" (Groupe de protection des personnes à l'égard du traitement des données à caractère personnel, DG XV D/5005/98final, du 22 avril 1998, "Vues préliminaires sur le recours à des dispositions contractuelles dans le cadre de transferts de données à caractère personnel vers des pays tiers", p. 7).

B les données concernées et leur utilisation

Il est intéressant de compléter cette première approche de l'objet du contrat par une analyse portant sur les types de données transférées.

A cet égard, il faut reprendre la distinction, classique, entre les données personnelles selon qu'elles sont ou non sensibles. On sait que la notion de données sensibles a été généralisée au niveau européen par la directive de 1995 : elles couvre l'origine raciale ou ethnique, les opinions politiques et convictions religieuses ou philosophique, l'appartenance syndicale et les données relatives à la santé. On peut ajouter à cela qu'on ne devrait manier qu'avec beaucoup de prudence, et qu'il serait donc judicieux d'identifier comme telles dans les contrats, les informations relatives aux mœurs, voire aux goûts, des personnes concernées, par exemple les consommateurs ou les salariés. Il y a là des données que l'on pourrait qualifier de "quasi-sensibles".

Les clauses contractuelles de transfert de données qu'on rencontre en pratique utilisent peu la notion de données sensibles. Le contrat-type du Conseil de l'Europe de 1992 n'y fait pas allusion (texte précité). En revanche, l'accord CEE-USA du 26 juillet 2000 les vise spécifiquement en précisant que les personnes concernées doivent avoir été mises en mesure de décider clairement si ces données peuvent être divulguées à un tiers (texte précité, rubrique "Choix")

Or, la distinction des contrats que l'on vient d'opérer pourrait se combiner de manière heureuse avec cette seconde distinction.

De fait, on s'avise que les contrats de confiance, du type du dépôt accessoire à une prestation de service, pourraient s'accommoder du transfert de données sensibles (avec sans doute des mesures de sécurité renforcées), précisément parce qu'ils reposent sur la confiance que l'exportateur de données peut avoir à l'égard de l'importateur. A l'inverse, puisqu'ils ne reposent pas sur la confiance, les contrats relevant de la catégorie de la cession d'informations ne devraient pas, en règle générale, pouvoir porter sur des données sensibles.

Ces observations montrent qu'il y aurait intérêt dans l'appréhension des clauses contractuelles de transfert de données personnelles vers des pays tiers à distinguer à la fois selon les types de contrats passés et selon les types de données concernées.

2° les engagements de l'exportateur

L'exportateur de données assume des obligations qui portent sur celles-ci (a), et des obligations à l'égard des personnes qu'elles concernent (b).

a) Obligations relatives aux données

S'agissant des données elles-mêmes, l'exportateur - outre le fait que les modèles de contrat prévoient généralement qu'il déclare avoir effectué le traitement de données dans des conditions de parfaite légalité - assume avant tout l'obligation d'informer l'exportateur sur le régime qui leur est applicable, notamment sur sa législation. De cette façon, ce dernier sera en mesure de savoir quelles sont les règles gouvernant, *ab initio*, le traitement des données.

Il serait heureux que les modèles de contrat prévoient également, sur ce plan, l'obligation pour l'exportateur de communiquer une copie de l'acte constitutif du traitement, par exemple la déclaration faite à l'autorité de contrôle : cela permettrait à l'exportateur de se faire une idée claire de la finalité du traitement, des destinataires des données, de leur durée de la conservation.

Au regard du droit commun des contrats, il faudra seulement prendre garde que cette communication puisse être faite dans le respect du secret des affaires.

b) Obligations envers les personnes concernées

L'exportateur de données assume aussi des obligations vis-à-vis des personnes concernées, car il importe que celles-ci puissent exercer leurs droits d'accès, de vérification et de rectification des données (V. infra, partie II). Une des obligations que l'exportateur assume, à cet égard, est d'inscrire, dans le contrat, une stipulation pour autrui destinée à ce que les personnes concernées puissent exercer leurs prérogatives à l'encontre de l'importateur (V. infra, partie II).

En application de la directive européenne de 1995, cependant, il semble qu'il s'impose à l'exportateur d'aller plus loin.

De fait, on l'a souligné (V. supra, en introduction), ce texte impose de recueillir le consentement de l'intéressé pour le traitement de données le concernant (art. 7), et prévoit qu'en cas de circulation des données il soit informé du transfert dont celles-ci font l'objet (art. 11 et 12). A supposer, donc, qu'initialement les personnes concernées aient donné leur accord pour la circulation des données, il semble bien qu'il faille leur notifier le transfert avant que ce dernier ne s'opère. Et l'obligation semble s'imposer avec d'autant plus de force qu'il s'agit, dans le cas de figure étudié, de transfert à destination de pays n'ayant pas un niveau de protection adéquat.

Dans cette perspective, les modèles de contrat devraient prévoir que l'exportateur a respecté son obligation de notifier aux intéressés le transfert des données par delà les frontières.

L'accord CEE-USA du 26 juillet 2000 prévoit, d'ailleurs, une obligation d'"informer les personnes concernées des raisons de la collecte et de l'utilisation des informations,... (et) des tiers auxquels ces informations sont communiquées", obligation qu'il convient d'exécuter, en cas de transfert de données personnelles, "avant qu'elles ne soient diffusées pour la première fois à un tiers" (texte précité, rubrique "Notification"), cette information devant permettre

aux intéressés d'exercer leur faculté de choix, c'est à dire le droit de refuser le transfert de données (texte précité, rubrique "Choix").

3° Les engagements de l'importateur

Tout comme l'exportateur, l'importateur de données assume des obligations qui portent sur celles-ci (a), et des obligations à l'égard des personnes qu'elles concernent (b).

a) Obligations relatives aux données

Dans les modèles contractuels en usage, l'importateur de données s'engage, tout d'abord, à respecter les règles gouvernant le traitement des données dans son pays d'origine, et cela conformément aux informations qui ont été portées à sa connaissance à ce propos.

Il contracte, notamment, les obligations de ne pas utiliser les données contrairement aux finalités du traitement, et de faire en sorte que des tiers non autorisés ne puissent pas y avoir accès.

Il s'engage, tout particulièrement à assurer, par des mesures techniques adaptées, la sécurité des données en cause, et il accepte que l'exportateur procède à des contrôles sur ce point dans son organisation (et V. sur ce point, infra B).

De telles obligations sont parfaitement acceptables au regard du droit commun des contrats.

B Obligations envers les personnes concernées

A l'égard des personnes concernées, l'importateur de données contracte l'obligation, non seulement de respecter la finalité du traitement et d'assurer sa sécurité, conformément au droit qui régit à l'origine sa constitution, mais aussi de satisfaire aux demandes émanant de ces derniers, par lesquelles ils réclameraient la possibilité d'user de leur droit d'accès, de vérification et de rectification.

Pour cela, il consent à leur égard, dans le contrat, une stipulation pour autrui (et sur l'efficacité de celle-ci, V. infra, partie II).

B. LES GARANTIES DE LA BONNE EXÉCUTION DU CONTRAT

Le contrat doit comporter des garanties de bonne exécution : préventivement, des moyens de contrôle permettent d'éviter les débordements (1°), et en cas de non-respect des engagements pris la sanction est la responsabilité des parties (2°).

Etant donné, comme on pourra le constater, la relative inadaptation du mécanisme de responsabilité, les moyens préventif prennent toute leur importance.

1° Le contrôle des moyens techniques de protection

Le dispositif préventif est généralement bien développé dans les contrats existants. Il est constitué par des moyens de contrôle de l'utilisation effective des données, au regard de la

finalité du traitement, et des mesures de sécurité devant être prises : ces moyens de contrôle sont à la disposition de l'exportateur, et s'exercent sur l'importateur.

Ce genre de mécanisme n'est, certes, pas fréquent dans les contrats de droit privé, mais on le rencontre parfois. De fait, certains accords commerciaux prévoient des possibilités de contrôle d'une partie sur l'activité de l'autre : ainsi sur la comptabilité (audit), le process de production (qualité), les éléments permettant l'établissement des prix (coût)...

Il n'y a donc aucune difficulté pour admettre la validité, et partant l'efficacité juridique du procédé. Il suffit que les modalités soient suffisamment précises pour qu'en pratique le dispositif fonctionne convenablement.

Ces mesures préventives devraient avoir pour intérêt d'éviter, autant que faire se peut, de recourir à des sanctions *a posteriori*.

2° La sanction de l'inexécution par la responsabilité

Dans les modèles contractuels existants, l'inexécution des obligations est sanctionnée, conformément aux principes généralement admis en droit des contrats (V. les principes Unidroit, précités, art. 7.4.1 et s.), par la possibilité d'obtenir des dommages-intérêts. On peut s'interroger, toutefois, sur l'adéquation de cette sanction.

a) Le mécanisme de la responsabilité

Comme sanction de la mauvaise exécution des obligations assumées par les parties, et notamment de celles de l'importateur des données, les contrats prévoient la possibilité de mettre en jeu la responsabilité de l'une ou l'autre des parties, voire des deux.

En pratique, ce sera généralement une personne concernée par les données qui trouvera matière à mettre en jeu cette responsabilité, parce qu'elle aura subi un préjudice. En ce cas, il conviendrait que les contrats soient clairs sur l'existence ou l'absence de solidarité, dans cette responsabilité entre exportateur et importateur : les modèles existants n'emploient pas toujours une terminologie satisfaisante (exemple : le projet CEE de clauses contractuelles, dans la version française, parle de responsabilité "conjointe", vraisemblablement pour signifier une responsabilité "solidaire"; et V. sur ce point, infra partie II).

Les dommages subis peuvent être divers : atteinte à la vie privée résultant de la divulgation de données confidentielles (par exemple : données de santé), refus d'une prestation sur le fondement d'informations inexactes (par exemple : réservation de chambre d'hôtel)...

Les personnes concernées, tiers au contrat passé entre l'exportateur et l'importateur, sont fondées à demander ainsi des dommages-intérêts sur le terrain contractuel en raison de la stipulation pour autrui que le contrat conscient à leur profit (V. infra partie II).

Eventuellement, l'exportateur des données pourra trouver à déclencher, lui aussi, une demande en dommages-intérêts, s'il éprouve un préjudice du fait de la mauvaise utilisation des données personnelles par l'importateur (par exemple : atteinte à l'image de l'entreprise du fait d'une "affaire" mettant en cause la diffusion de ces données).

b) L'adéquation de la sanction

On doit toutefois souligner que la responsabilité contractuelle, et l'allocation de dommages-intérêts qu'elle justifie, est un mécanisme assez mal adapté à la situation.

De fait, en la matière, le préjudice sera souvent diffus, difficile à prouver dans son existence ou dans son étendue, et ses causes seront souvent mal identifiées... Il ne sera pas rare, d'ailleurs que l'utilisation des informations dans des conditions contraires au contrat, ou la défaillance des mesures de sécurité ait des conséquences qui restent assez longtemps inconnues des personnes concernées.

En outre, on peut se demander si la simple menace de devoir réparer le préjudice causé est suffisamment dissuasive pour limiter les dysfonctionnements.

La comparaison avec ce qui se passe dans l'ordre interne, dans le cadre du pays de l'exportateur, est à cet égard instructif : le traitement de données fait l'objet d'une notification à l'autorité de contrôle; celle-ci dispose de moyens d'investigation lui permettant de constater la violation du dispositif légal (sur l'impossibilité de procéder ainsi avec l'importateur de données, V. infra partie II); en cas d'infraction des sanctions pénales sont généralement encourues...

Tout cela permet d'assurer un certain respect des contraintes juridiques et offre la possibilité de sanctionner les écarts de conduite, *a priori*, en dehors même de tout préjudice particulier causé aux personnes concernées.

Sensible est donc la différence existant dans les moyens de mise en œuvre des règles de protection des données selon qu'on reste à l'intérieur d'un ou plusieurs pays où est assuré un niveau adéquat de protection, ou qu'on comble le déficit de protection d'un pays tiers par le recours aux clauses contractuelles.

C. LE DÉNOUEMENT DU CONTRAT

Le dénouement du contrat est différent selon qu'on se rattache à un contrat de dépôt accessoire à une prestation de service ou qu'on est dans un schéma du type de la cession d'informations.

Dans la première hypothèse, le contrat s'échelonne dans le temps, souvent sur une période assez longue. Le dénouement consacre la fin des relations de sous-traitance et, normalement, se marque par une restitution de ce qui a été confié - ou s'agissant de données informatisées par la destruction de celles-ci, ce qui est équivalent.

Dans la seconde hypothèse, le contrat est souvent à exécution immédiate, ou du moins il peut avoir une durée assez limitée. En tout cas, l'exportation de données a une allure définitive : l'importateur a contracté pour que les données lui soient cédées, et pour pouvoir en faire l'usage qu'il souhaite. Certes, il assume des obligations générales relatives aux données, notamment de respecter la finalité du traitement initialement déclarée. Mais la fin du contrat ne donne pas lieu à restitution des données, en général.

Enfin, il peut être utile, quelque soit le cas de figure, que l'accord des parties envisage l'après-contrat : notamment, les obligations pouvant subsister (confidentialité, sécurité...), ainsi que les réclamations pouvant surgir postérieurement.

II. LE CONTRAT DE TRANSFERT DE DONNÉES ET LES RAPPORTS AVEC LES TIERS

Dans les contrats de transfert de données, un certain nombre de tiers peuvent se trouver en cause : les personnes concernées par les données, au premier chef (A), les tiers vers lesquels les données seraient réexportées par l'importateur, ensuite (B), les autorités de contrôle nationales sous la juridiction desquelles se trouvent les données, enfin (C).

On le constatera, le fait qu'il s'agisse de tiers au contrat de transfert de données, ou simplement de tiers au pays d'origine des données, peut soulever des difficultés de mise en œuvre du mécanisme contractuel.

A. LES PERSONNES CONCERNÉES PAR LES DONNÉES

La situation des tiers concernés par les données est originale : ils sont au centre du dispositif, le contrat étant principalement fait pour assurer leur protection, alors que le pays vers lequel vont être acheminées les données n'est pas suffisamment protecteur de leurs intérêts. Il est donc essentiel pour l'efficacité du dispositif qu'ils puissent se prévaloir de droits en vertu du contrat en cause. Cela est assuré par un mécanisme juridique, celui de la "stipulation pour autrui".

A ce procédé de nature contractuelle, dont on va apprécier le fonctionnement, doivent s'ajouter des mesures, protectrices des personnes concernées, tirées du droit des données personnelles : le traitement de données doit avoir été déclaré comme pouvant faire l'objet d'un transfert vers l'étranger (destinataires des données); et, en vertu de la directive de 1995, il semble s'imposer que les personnes concernées aient consenti à un tel transfert, ou, pour le moins, on doit leur avoir notifié cette éventualité (et V. supra, partie I).

Pour s'en tenir au terrain contractuel, on soulignera que le recours à la stipulation pour autrui souffre de ce que la notion n'est pas universellement admise (1°). Mais, dans la mesure où elle peut jouer, cette notion permet aux personnes concernées de demander au promettant, en l'occurrence l'importateur des données, l'exécution des obligation prévues au contrat (2°).

1° La stipulation pour autrui en faveur des personnes concernées

La stipulation pour autrui est une promesse, faite par une partie au contrat, le plus souvent en échange de ce qui est assumé envers elle par l'autre partie, de fournir une prestation à un tiers. Le mécanisme est, par exemple, utilisé dans le domaine de l'assurance : assurance pour le compte de qui il appartiendra (couvrant une marchandise en cours de transport, alors qu'elle peut faire l'objet de ventes successives pendant ce temps : le bénéfice en reviendra à celui qui est propriétaire lors de l'avarie), assurance sur la vie (au profit du conjoint survivant, ou d'enfants nés ou à naître)...

Dans les contrats de transfert de données personnelles, l'importateur prend un certain nombre d'engagements envers l'exportateur, notamment en matière de sécurité, mais également envers les tiers : il s'oblige, en particulier à répondre aux demandes d'accès, de vérification et de rectification provenant des personnes concernées.

L'efficacité de ce type d'engagement dépendra du droit applicable au contrat.

La stipulation pour autrui, en effet, est admise dans certains droits des pays européens, comme le droit français et le droit allemand, mais elle ne l'est pas dans tous : le droit anglais, notamment, l'ignore (V. sur ce point, T. Weir, An introduction to comparative law, 2nd ed. 1987, T. II, p. 145 s. pour le droit allemand, 148 s. pour le droit français et 151 s. pour le droit anglais). En raison de cette divergence, on ne trouve pas mentionnée la stipulation pour autrui dans les principes applicables aux contrats internationaux adoptés par Unidroit (précités).
Le raisonnement suivi par les juristes anglais, par exemple, est que le contrat ne peut pas être étendu en dehors du cercle des parties ("privity") et qu'un tiers, ne fournissant aucune contrepartie ("consideration"), ne saurait avoir de droits en vertu du contrat.

En revanche, ceux qui admettent la stipulation pour autrui se fondent pour cela sur la liberté contractuelle, l'absence de préjudice causé au tiers (la stipulation leur bénéficie) et les avantages pratiques du mécanisme.

Le système des contrats de transfert de données, reposant sur des engagements pris par des entreprises destinatrices envers, notamment, les personnes concernées, n'est donc pas efficace juridiquement dans tous les droits européens.

2° Les droits des personnes concernées en vertu de la stipulation pour autrui

Lorsque la loi applicable - et l'on a vu que le contrat devrait prévoir qu'est compétente la loi du pays de l'exportateur des données - admet la stipulation pour autrui, ce dernier acquiert des droits en vertu du contrat auquel il est tiers. En l'occurrence, ce sont les personnes concernées par les données transférées qui vont acquérir des droits.

Il peut s'agir de droits à l'exécution en nature (en droit anglais, "specific performance", ou "performance in kind") si, là encore, la loi applicable admet ce type d'exécution du contrat (a). Sinon c'est un droit à des dommages-intérêts (b), dont on a déjà évoqué le principe en soulignant que ce type de sanction ne présente sans doute pas pas l'efficacité souhaitable (V. supra partie I), et dont il reste à préciser qu'elle peut être soit une responsabilité solidaire entre l'exportateur et l'importateur, soit une responsabilité conjointe (c).

a) L'exécution en nature : accès, vérification et droit à rectification

La première chose que peut souhaiter la personne concernée est d'obtenir, comme dans son propre pays, que lui soient effectivement ouverts les droits d'accès, de vérification et de rectification des données la concernant. L'importateur s'y engage dans les contrats en usage pour les transferts de données.

Il n'y a pas de difficulté si l'importateur accepte de remplir ses engagements et donne effectivement la possibilité à la personne concernée d'exercer ces droits. Mais, au cas où il y a une résistance de sa part, la question se pose de savoir si l'on peut obtenir de lui, par suite d'une injonction obtenue en justice, qu'il y consente.

A cet égard, on rencontre à nouveau un obstacle en droit anglais, où l'exécution en nature n'est généralement pas admise (V. sur le sujet, T. Weir, précité, p. 169 s.), alors que la solution est admise en Allemagne et en France. Encore qu'on pourrait faire valoir en droit français une certaine tendance jurisprudentielle, qui s'est récemment affirmée, à faire jouer,

contrairement à l'opinion dominante, l'art. 1142 c. civ. selon lequel les obligations de faire ou de ne pas faire se résolvent en dommages-intérêts.

En principe, toutefois, la majorité des pays européens admettent l'exécution en nature des contrats, et si l'on combine ce principe avec l'efficacité de la stipulation pour autrui, il apparaît qu'en pur droit les personnes concernées pourraient, le plus souvent, obtenir en justice que l'importateur des données leur permettent d'exercer les droits d'accès, de vérification et de rectification des informations recueillies à leur sujet.

b)La responsabilité : sanction des engagements pris et réparation du préjudice subi

A défaut d'être satisfait par l'exercice de ces droits, ou s'il souffre d'ores et déjà un préjudice, le tiers concerné pourra rechercher la responsabilité de l'exportateur ou de l'importateur des données. Ce droit, dans une certaine mesure, en ce qui concerne l'importateur, est subordonné à ce que la loi applicable admettre cette recherche de responsabilité d'un contractant par un tiers : tel est le cas dans les pays qui reconnaissent la validité de la stipulation pour autrui (V. supra 1°).

On a déjà relevé que ce mécanisme peut paraître d'une efficience faible pour gager le bon fonctionnement d'un système de protection des données où sont en jeu des exigences tenant aux informations en cause, à la finalité de traitement ou aux destinataires des informations (V. supra, partie I).

Le droit aux dommages-intérêts reste néanmoins un mécanisme incontournable s'agissant de la réparation du préjudice subi. Il se posera toutefois, alors, des questions touchant à la loi applicable à l'action.

La stipulation pour autrui semblerait recommander le droit du contrat, et donc en principe, comme on l'a suggéré, la loi du lieu d'établissement de l'exportateur du traitement, qui coïncidera souvent avec celle du domicile de la personne concernée (salarié de l'entreprise, client dans le pays...). Il se peut néanmoins que, s'agissant de dommage causé à la personne, et non de préjudice économique, on puisse faire valoir dans certains pays européens un rattachement à la responsabilité extracontractuelle. Or, en la matière, solution universellement admise, la loi applicable est celle du lieu du délit : ce sera aussi bien celle du lieu où ce dernier a été commis (chez l'importateur), que celle du lieu où il a été subi (chez la victime)... Avec des résultats différents selon le choix que l'on fait.

Ce qui rend la question aiguë est que les régimes de responsabilité ne sont pas identiques dans tous les pays : certains n'admettent qu'avec réticence la réparation du préjudice moral, et en tout état de cause ce type de dommage peut être difficile à invoquer sur un terrain contractuel... Or, les infractions aux règles de traitement des données personnelles peuvent provoquer des préjudices de cet ordre.

c) Les modalités de la responsabilité : responsabilité conjointe ou solidaire

Un autre point à évoquer, que les contrats en usage n'envisagent pas toujours de façon claire, concerne la manière dont exportateur et importateurs vont être tenus pour responsables du dommage causé à une personne concernée par les données : conjointement, ou solidairement.

En partie, la difficulté vient de la différence de vocabulaire d'un droit à un autre. Ainsi, ce que les juristes français appellent être "solidairement responsable", se dit en anglais "jointly and severabily liable".

Toujours est-il que deux solutions sont envisageables et qu'il faut faire un choix clair. La première est celle de la responsabilité simplement "conjointe" : chacun des deux intervenants est responsable, de son côté, des dommages qu'il cause, et l'un n'est pas responsable pour l'autre, en cas d'insolvabilité. En revanche, si la responsabilité est "solidaire", chacun des intervenants, importateur et exportateur, répondra, en plus des dommages qu'il a cause, du dommage causé par l'autre, et devra notamment en assurer la réparation au cas où l'autre ne le ferait pas.

La seconde solution est, à l'évidence, plus favorable aux personnes concernées et il semble que, pour leur assurer la meilleure protection, par un mécanisme qui se révèle déjà assez faible pour y parvenir, le mieux est de retenir la solution de la responsabilité solidaire.

B. LES DESTINATAIRES D'UNE RÉEXPORTATION DES DONNÉE

Si l'on admet que les données personnelles objet d'un transfert peuvent, à nouveau, être transférées vers un autre pays, les destinataires de cette réexportations constituent des tiers qui entretiennent des relations de proximité avec le contrat initial de transfert.

Le principe même d'un tel transfert peut, certainement, être discuté (a) et, si l'on répond par l'affirmative, ses modalité doivent être sérieusement encadrées (b).

1° La possibilité de réexportation

La difficulté surgit au cas où le second transfert s'opère, également, à destination d'un pays dont le niveau de protection ne serait pas adéquat. En ce cas, tout repose à nouveau sur la protection contractuelle. Or, on voit en l'occurrence s'accroître les risques encourus par les personnes concernées, et que la perspective, pour elles, de pouvoir invoquer à l'encontre du nouveau destinataire des données des droits contractuels s'amenuise.

Le second destinataire des données est, en effet, un tiers au contrat ayant organisé, initialement, le transfert de celles-ci vers l'étranger. Et, par là-même, la créance que les personnes concernées tirent de la stipulation pour autrui insérée dans ce contrat à leur profit n'est pas, *de plano*, invocable à l'encontre du nouveau destinataire. Il faut, pour que l'on puisse faire valoir un droit contractuel à son encontre, que le second contrat de transfert de données contienne, lui aussi, une stipulation pour autrui... On perçoit que le système contractuel, en même temps qu'il se complique, se fragilise.

Et cela d'autant plus qu'une difficulté supplémentaire apparaît qui tient à la détermination de la loi applicable à ce second contrat : il serait judicieux de le soumettre au même droit que le contrat initial, dont on a proposé qu'il soit régi par la loi du pays de l'exportateur, mais celle-ci serait une loi tierce par rapport à l'importateur et au nouveau destinataire des données...

Il serait donc recommandé de limiter le plus possible, voire d'interdire, de telles réexportations de donnés, notamment s'agissant de données sensibles, ou quasi-sensibles.

On voit pourtant certains modèles contractuels l'admettre, sans guère de restrictions. Ainsi, l'avant-projet de décision de la CEE sur les clauses-type pour le transfert des données à caractère personnel vers des pays tiers, de septembre 2000, prévoit cette possibilité, en précisant seulement que le nouveau transfert n'est possible qu'avec l'accord écrit de

l'exportateur de données (texte précité, art. 6, h). Et dans l'accord CEE-USA du 26 juillet 2000 une telle réexportation est également admise moyennant un certain nombre de précautions (texte précité, rubrique "Transfert ultérieur").

2° Les conditions de la réexportation

Il faut envisager les conditions de la réexportation sous deux angles : dans le contrat initial et dans le contrat second.

Dans le contrat initial, on prévoiera que l'importateur des données ne pourra les réexporter sans faire en sorte que le nouveau destinataire des informations assume les mêmes engagements que lui, tant en ce qui concerne la sécurité et le respect de la finalité du traitement, que dans les rapports avec les personnes concernées (accès, rectification...).

Dans le contrat second, on réitèrera ces engagements et on inscrira une stipulation pour autrui au profit des personnes concernées. L'efficacité de celle-ci souffrira, toutefois, des mêmes aléas juridiques que l'on a pu déjà constater en examinant ce mécanisme, en raison du fait que certains droits ne la reconnaissent pas (V. supra).

Sans doute le plus sûr serait d'inscrire dans le premier contrat un modèle pour le second contrat, ce qui permettra d'en bien maîtriser le contenu. Dans ce modèle serait traité la délicate question de la loi applicable.

C. LES AUTORITÉS DE CONTRÔLE DES DONNÉES

Une dernière catégorie de tiers, enfin, doit être évoquée : les autorités de contrôle des données.

Celles-ci se trouvent dans une position délicate à l'égard des transferts de données vers des pays n'ayant pas un niveau de protection adéquat du fait que, dans le système exclusivement contractuel, elle se voient privées à l'égard d'un détenteur des données, en l'occurrence l'importateur, des pouvoirs qui leur sont traditionnellement dévolus : investigation, enquête, injonction, action en justice... De fait, il s'agit de pouvoirs ou prérogatives ressortissant aux lois de police, qui ont une portée limitée au territoire national.

Ces pouvoirs, en tout état de cause, ne pourront guère être exercés qu'en direction de l'exportateur des données, situé sur le territoire national où siège l'autorité, ou par son intermédiaire.

Dans les commentaires assortissant certains modèles contractuels, cette observation est faite. Ainsi, dans le document "Outsourcing and privacy", émanant du Privacy Advisory Commitee du Royaume-Uni, document à l'intention du Commonwealth (précité, 1994), où il est précisé que dans les hypothèses d'exportation de données : "There is usualy and necessarily a substantial reduction in the control that an agency has over how the service is provided on a day-to-day basis".

III. LE CONTRAT DE TRANSFERT DE DONNÉES ET LA RÉSOLUTION DES LITIGES

Comme dans tous contrats internationaux, les clauses relatives aux litiges ont leur importance. Elles ont aussi leurs faiblesses.

Dans les modèles en usage, on rencontre des clauses prévoyant, ainsi, la loi applicable, le tribunal compétent, et, souvent aussi, mettant en place une procédure d'arbitrage.

Ces modalités ont une efficacité dans les rapports entre les parties (A), mais n'ont qu'une portée très limitée dans les rapports avec les tiers (B), qui sont pourtant au centre au dispositif.

A. LES LITIGES ENTRE LES PARTIES

Dans les rapports entre les parties, que sont les exportateur et importateur de données, il est souhaitable de prévoir la loi applicable et le tribunal compétent. On peut également s'en remettre à l'arbitrage.

On a déjà souligné, s'agissant de la loi applicable, qu'il serait judicieux de choisir celle du pays d'origine des données, c'est-à-dire d'un pays européen, parce qu'il doit disposer d'un niveau adéquat de protection des données (V. supra, en introduction).

On observera, toutefois, qu'il ne paraît guère admissible, au regard des règles de procédure et notamment du respect des droits de la défense, de faire figurer dans un modèle de contrat, comme l'envisage l'avant-projet de décision de la CEE sur les clauses-type pour le transfert des données à caractère personnel vers des pays tiers, de septembre 2000, une clause aux termes de laquelle l'importateur de données s'engagerait à accepter toute décision rendue par l'autorité de contrôle des données, ou une juridiction, dans le pays d'origine de celles-ci (texte précité, art. 9, §2).

On a pu noter également que, si le contrat prévoit la possibilité pour l'importateur de données d'en effectuer la réexportation vers un autre pays tiers, il se pose un second problème de détermination de la loi applicable, à propos de ce nouveau transfert, et qu'il serait souhaitable de soumettre l'ensemble contractuel à une législation unique : celle du pays d'origine première des données (V. supra, partie II).

Mais ce n'est pas dans les rapports entre les parties que les litiges sont le plus à redouter.

B. LES LITIGES AVEC LES TIERS

Dans les rapports avec les tiers, les clauses relatives aux litiges risquent d'avoir une efficacité très réduite. Les tiers, en effet, ne sont pas obligés par les dispositions que les parties ont prévues pour elles. La détermination de la loi applicable, ou celle du tribunal compétent, pourra donc difficilement être imposée, par exemple, aux personnes concernées par les données, à l'occasion d'un contentieux.

On pourrait, certes, soutenir que les personnes concernées ne sauraient invoquer à leur profit la stipulation pour autrui que contient le contrat sans respecter en même temps les clauses concernant le règlement des différends. Toutefois, le tiers victime d'un dysfonctionnement dans la protection des données pourra récuser aisément cet argument en déclarant fonder son action, non pas sur le contrat, mais sur la responsabilité extracontractuelle et la faute commise à son encontre.

Le même raisonnement vaut à l'égard des clauses d'arbitrage. Elles ne sauraient lier les tiers, notamment les personnes concernées. Et si l'on souhaite recourir à ce mode de règlement des litiges, il faudra le faire sur la base d'un compromis passé entre les responsables des données et la victime, une fois le litige né.

CONCLUSION GÉNÉRALE

L'analyse des possibilités d'appréhension du phénomène de transfert international de données personnelles par voie de clauses contractuelles, au regard notamment du droit des obligations, a permis de montrer un certain nombre de faiblesses de ce dispositif.

D'une part, on observe que, même si les obligations généralement insérées dans les modèles de contrats permettent de donner quelques assurances quant à la sécurité des données et au respect d'un certain nombre de principes (finalité, accès, rectification...), le procédé de la stipulation pour autrui, indispensable pour autoriser les personnes concernées à exercer leurs droits, présente des faiblesses en raison du fait que certains systèmes juridiques ne la reconnaissent pas, et qu'au cas de réexportation des données vers un second pays tiers, la nécessité de dédoubler la stipulation pour autrui rend le système passablement complexe.

D'autre part, et surtout, on a pu constater que le mécanisme du contrat est assez mal adapté pour garantir l'efficacité de règles qui relèvent avant tout de la catégorie des lois de police, dont le respect devrait pouvoir être assuré par des autorités de contrôle susceptibles d'investiguer et de sanctionner, alors que sur le terrain du droit des obligations, la sanction des écarts de conduite des détenteurs des données est constituée essentiellement par la possibilité pour les personnes concernées, au cas où elles souffrent un préjudice, d'en obtenir la réparation grâce à l'allocation de dommages-intérêts.

_____

Jérôme Huet
Professeur de droit
Le 30. 10. 2000