Les autorités européennes de protection des données à caractère personnel viennent de publier un document de travail sur le conflit de droits entre les *pre-trial discovery rules* (1) et la protection des données à caractère personnel. Faisant suite à un précédent article sur ce thème (2), Mes Olivier Proust et Cédric Burton analysent la position commune des autorités européennes et présentent les défis à venir.

Les autorités européennes prennent position sur le conflit de droits entre les règles de *e-discovery* et la protection des données à caractère personnel (3)

Par Olivier PROUST
Avocat au Barreau de Paris
Hunton & Williams

Par Cédric BURTON
Avocat au Barreau
de Bruxelles
Hunton & Williams

Le Groupe de travail de l'article 29 (4) (ci-après « *GT 29* ») a publié, le 11 février 2009, un document de travail relatif à l'application des règles de *pre-trial discovery* (5) dans les litiges civils internationaux, et aborde la question du conflit de droits entre les règles de *e-discovery* anglo-saxonnes et la protection des données à caractère personnel en Europe (6). Très attendu par les spécialistes de la protection des données à caractère personnel, ce document de travail contient non seulement une description précise des enjeux liés à la problématique de *e-discovery* mais également une série de lignes directrices destinées aux entreprises confrontées à ce problème.

Dans son document de travail, le GT 29 décrit de façon détaillée le concept de *pre-trial discovery* et explique les différences entre les règles de procédure civile des pays de *Common Law* et celles des pays de tradition civiliste. Selon le GT 29, les parties à un litige (7) ont un intérêt légitime à collecter les documents et les informations nécessaires au soutien de leurs prétentions. Toutefois, les parties doivent également respecter les droits des personnes dont les données personnelles sont communiquées dans le cadre du litige, conformément aux règles européennes de protection des données à caractère personnel. Ainsi, le GT 29 constate l'existence d'intérêts divergents et admet qu'il faut trouver un terrain d'entente entre deux systèmes juridiques différents. Nous ne reviendrons pas de manière approfondie sur le contexte juridico-politique entourant la question de *e-discovery*, cette question ayant déjà été traitée dans notre article précédent (8).

L'intérêt principal du document de travail du GT 29 porte sur l'énoncé de lignes directrices destinées à aider les sociétés européennes à concilier les impératifs d'un litige civil en cours dans un pays de *Common Law* avec les obligations d'un responsable de traitement situé en Europe (I). Il conviendra, ensuite, de souligner le champ d'application restreint de ce document de travail (II) et de s'interroger sur les suites à donner à ce conflit de droits (III).

I. – ANALYSE DES LIGNES DIRECTRICES PROPOSÉES PAR LE GT 29

Le GT 29 distingue quatre étapes dans la mise en œuvre des *pre-trial discovery rules* :
– la conservation ;
– la communication ;
– les transferts ultérieurs ;
– les usages secondaires.

Selon le GT 29, chacune de ces étapes peut donner lieu à un traitement de données à caractère personnel. Dès lors, la question de *e-discovery* doit s'analyser au regard de ces différentes étapes et il convient de s'assurer, lors de chacune d'entre elles, que les traitements mis en œuvre respectent la ou les législations >

(1) Règles de procédure civile existant dans les pays de *Common Law* et qui se fondent sur une mise en état de l'affaire par les parties au litige (pour plus d'informations, voir note 2). **(2)** Voir Proust O. et Burton C., Le conflit de droits entre les règles américaines de *e-discovery* et le droit européen de la protection des données à caractère personnel… entre le marteau et l'enclume, RLDI 2009/46, n° 1531. **(3)** Les propos tenus dans le présent article n'engagent que les auteurs et pas l'institution à laquelle ils appartiennent. Les auteurs peuvent être contactés à l'adresse suivante : cburton@hunton.com et oproust@hunton.com. **(4)** Groupe de protection des personnes à l'égard du traitement des données à caractère personnel, regroupant les autorités de protection des données personnelles des 27 pays membres de l'Union européenne. **(5)** Dans un souci de clarté, les expressions « *pre-trial discovery* » et « *e-discovery* » sont utilisées de manière synonyme. **(6)** Voir « *Working Document 1/2009 on pre-trial discovery for cross border civil litigation* », adopté le 11 février 2009, disponible en anglais sur le site suivant : <http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2009_en.htm>. **(7)** Nous rappelons qu'il n'est pas question ici des litiges entre ressortissants de l'Union européenne, lesquels sont soumis au Règlement n° 1206/2001 du Conseil du 28 mai 2001 relatif à la coopération entre les juridictions des États membres dans le domaine de l'obtention de preuves en matière civile ou commerciale. **(8)** Voir note 2.

nationales relatives à la protection des données à caractère personnel. Ainsi, l'application des règles de *e-discovery* en Europe ne soulève pas seulement la question du transfert des données vers l'étranger mais porte plus généralement sur la mise en conformité de l'ensemble des traitements antérieurs au transfert (collecte, conservation, analyse, etc.) avec les règles européennes de protection des données à caractère personnel. À ce titre, le GT 29 retient sept principes issus de la directive 95/46/CE (9) qui méritent une attention particulière.

A. – La légitimité du traitement

Afin de mettre en œuvre les règles de *pre-trial discovery* de manière loyale et licite, le traitement de données à caractère personnel doit être réalisé de manière légitime et doit, à ce titre, se fonder sur l'une des bases légales énoncées à l'article 7 (10) de la directive 95/46/CE. Selon le GT 29, trois bases légales peuvent justifier le traitement de données à des fins de *e-discovery*. En premier lieu, sans l'écarter totalement, le GT 29 se prononce en défaveur du consentement des personnes concernées comme base légale pour le traitement (11) en raison des difficultés pratiques liées au respect des conditions de validité du consentement (12). En effet, dans le contexte de *e-discovery*, il est souvent difficile d'informer toutes les personnes concernées, y compris les consommateurs ou fournisseurs, sur le traitement et le transfert de leurs données vers une juridiction étrangère. De plus, en raison du lien de subordination qui existe entre un employeur et ses salariés au sein de l'entreprise, le consentement des salariés ne peut être considéré comme étant donné librement (13). Enfin, la personne concernée par un traitement doit être libre de retirer son consentement à tout moment, sans risque de sanction, ce qui est souvent difficile lorsque les données ont été communiquées à la partie adverse.

S'agissant du respect d'une obligation légale à laquelle le responsable du traitement est soumis (14), le GT 29 considère que cette base légale ne peut s'appliquer en l'espèce parce que les demandes de *e-discovery* reposent sur une disposition légale ou réglementaire étrangère. Or, cette exception s'entend uniquement d'une obligation légale nationale. Néanmoins, le GT 29 reconnaît qu'il existe dans certains États membres une obligation légale de respecter les injonctions prononcées par une juridiction étrangère et admet, dans ce cas, que le traitement puisse être légitime.

> Le GT 29 présente le principe de proportionnalité comme étant l'élément principal permettant de garantir un équilibre entre les intérêts en cause.

Enfin, s'agissant de savoir si le traitement de données est nécessaire à la poursuite d'un intérêt légitime (15), le GT 29 précise que les impératifs d'un litige en cours peuvent être légitimes mais ne doivent néanmoins pas porter atteinte aux droits et aux libertés des individus. Ainsi, le responsable du traitement doit trouver un équilibre entre, d'une part, les intérêts des parties à obtenir les informations et les documents au soutien de leurs prétentions et, d'autre part, les intérêts des personnes dont les données sont divulguées au cours de ce litige, notamment les intérêts des tiers à la procédure. À cet égard, il convient d'appliquer le principe de proportionnalité, et de tenir compte de la pertinence des données communiquées et des risques d'atteinte à la vie privée des personnes concernées.

B. – Le respect du principe de proportionnalité

Le GT 29 présente le principe de proportionnalité (16) comme étant l'élément principal permettant de garantir un équilibre entre les intérêts en cause. Selon le GT 29, le responsable du traitement a le devoir de filtrer les données qui sont divulguées à la partie adverse, le but étant de communiquer les seules données objectivement utiles au litige. En principe, ce travail de filtrage devrait être réalisé dans le pays d'origine des données (c'est-à-dire en Europe). Le GT 29 recommande pour cela de faire appel à un tiers de confiance qui aura pour mission d'analyser les données de manière objective et indépendante, et de déterminer leur pertinence au regard du litige en cours.

Lorsque l'identité des personnes concernées par le traitement ne constitue pas un élément indispensable du litige, le GT 29 recommande d'anonymiser ou de pseudonymiser les données. Ce procédé permet ainsi de transférer à la partie adverse les informations jugées pertinentes durant la phase de *pre-trial discovery*, tout en préservant l'anonymat des individus, et laisse le soin au tribunal étranger de juger ultérieurement si l'identité d'une personne est une information nécessaire pour le litige en cours. Le cas échéant, le responsable du traitement devrait se rapprocher du tribunal saisi de l'affaire afin d'expliquer les règles applicables en Europe et tenter de restreindre le champ de la procédure, autant que possible.

Le principe de proportionnalité impose également au responsable du traitement de mettre en œuvre une politique de conservation des données (17). Au regard du droit européen, la conservation, la rétention ou l'archivage de données en vue d'un litige constitue un traitement de données à caractère personnel. Il n'est donc pas possible de conserver toutes les données pour une durée indéterminée afin d'anticiper un litige. En revanche, lorsqu'un litige particulier a débuté, les données pertinentes doivent être conservées jusqu'à la fin de la procédure, y compris la procédure en appel, au risque de violer les règles de *pre-trial discovery* (18). De même, si une procédure a commencé dans un pays de *Common Law* (par exemple, aux États-Unis) et qu'une entreprise est soumise à une procédure de *litigation hold* (19), le GT 29 admet

---

(9) 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. **(10)** Article 7 de la directive 95/46/CE : « *Les États membres prévoient que le traitement de données à caractère personnel ne peut être effectué que si : (a) la personne concernée a indubitablement donné son consentement ; ou (b) il est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci ; ou (c) il est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis ; ou (d) il est nécessaire à la sauvegarde de l'intérêt vital de la personne concernée ; ou (e) il est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique, dont est investi le responsable du traitement ou le tiers auquel les données sont communiquées ; ou (f) il est nécessaire à la réalisation d'un intérêt légitime poursuivi par le responsable du traitement ou par le ou les tiers auxquels les données sont communiquées, à condition que ne prévalent pas l'intérêt ou les droits et libertés fondamentaux de la personne concernée, qui appellent une protection au titre de l'article 1er paragraphe 1* ». **(11)** Voir article 7(a) de la directive 95/46/CE. **(12)** D'après l'article 2(h) de la directive 95/46/CE, le consentement de la personne concernée n'est valable que s'il est libre, spécifique et informé. **(13)** Selon le Groupe de travail de l'article 29, le consentement ne peut pas être donné librement dans un contexte professionnel (pour plus d'informations, voir l'avis 8/2001 du GT 29 sur le traitement des données à caractère personnel dans le contexte professionnel, adopté le 13 septembre 2001). **(14)** Voir article 7(c) de la directive 95/46/CE. **(15)** Voir article 7(f) de la directive 95/46/CE. **(16)** Conformément à l'article 6 de la directive 95/46/CE, les données doivent être collectées pour des finalités déterminées, explicites et légitimes, et ne peuvent être traitées ultérieurement de manière incompatible avec ces finalités. Les données doivent également être adéquates, pertinentes et non excessives. **(17)** Voir article 6(e) de la directive 95/46/CE. **(18)** C'est ce que l'on appelle en procédure civile américaine « *spoliation* » (pour plus d'informations, voir note 2). **(19)** Procédure par laquelle les entreprises qui sont parties à un litige se voient obligées de préserver les documents pouvant se révéler pertinents pour le litige en cours ou à venir.

qu'une entreprise puisse suspendre sa politique de conservation des documents afin de répondre à cette obligation.

C. – L'application de restrictions particulières

Certaines catégories de données sont soumises à des restrictions particulières dans chaque État membre. Il en est ainsi des données sensibles (20) qui requièrent soit le consentement de la personne concernée, soit l'existence d'une autre base légale (comme la constatation, l'exercice ou la défense d'un intérêt en justice) (21) pour pouvoir être traitées. De plus, certaines catégories de données (par exemple, les données de santé ou les informations détenues par un avocat) sont protégées par le secret professionnel qui interdit en principe leur divulgation à des tiers. Enfin, certaines dispositions légales ou réglementaires peuvent également s'opposer à la communication des données (par exemple, le secret des correspondances et des communications électroniques).

D. – L'information des personnes concernées

En principe, les personnes concernées doivent être informées au moment de la collecte de leurs données (22). Le GT 29 considère que le responsable du traitement devrait informer les personnes concernées à deux reprises : une information générale précisant que les données pourront être communiquées à l'étranger dans l'éventualité d'un litige et une information spécifique lorsque le litige commence. Par ailleurs, dans le contexte de *pre-trial discovery*, les données peuvent être collectées ou détenues par un tiers, par exemple, par l'une des parties au litige ou par l'une de ses filiales. Dans ce cas, le responsable du traitement doit informer les personnes concernées dans un délai raisonnable suivant la mise en œuvre du traitement. Enfin, dans certains cas limités, l'information des personnes concernées peut être différée si cela risque de compromettre la procédure ou l'obtention des preuves. Cette exception doit néanmoins s'appliquer au cas par cas et de manière restrictive (23).

E. – Le respect des droits des personnes concernées

Le responsable du traitement doit s'assurer que les personnes concernées ont les moyens d'exercer leurs droits (24), notamment le droit d'accéder et de rectifier les données erronées, incomplètes ou périmées. Les personnes concernées peuvent également s'opposer au traitement des données les concernant à condition d'invoquer un ou plusieurs motifs légitimes qui tiennent à leur situation particulière (25). Le GT 29 précise que les parties peuvent exercer leurs droits à tout moment de la procédure et ne peuvent pas y renoncer. Le responsable du traitement en Europe est responsable de la mise en œuvre de ces droits et encourt des sanctions en cas de non-respect de cette obligation.

Dans le contexte de *pre-trial discovery*, les données peuvent être collectées ou détenues par un tiers, par exemple, par l'une des parties au litige ou par l'une de ses filiales.

F. – La sécurité des données

Le GT 29 rappelle que le responsable du traitement doit prendre toutes les mesures techniques, administratives et organisationnelles appropriées pour garantir la sécurité des données contre la destruction accidentelle ou illicite, la perte accidentelle, l'altération, la diffusion ou l'accès non autorisés de celles-ci. Ces mesures doivent être proportionnées aux finalités du traitement, à la sensibilité des données traitées, aux risques prévisibles et à l'état de l'art, conformément aux dispositions applicables dans les différents États membres. Ces mesures de sécurité s'imposent non seulement au responsable du traitement mais également aux cabinets d'avocats impliqués dans la procédure, ainsi qu'à tous les services administratifs, experts et tiers désignés pour collecter et analyser les documents et les informations.
Le responsable du traitement doit également veiller à ce que les sous-traitants respectent les principes énoncés dans la directive 95/46/CE et traitent les données uniquement pour les finalités spécifiques pour lesquelles elles ont été collectées. De plus, les sous-traitants ne peuvent agir que sur instruction du responsable du traitement et doivent être soumis à une obligation de confidentialité. Enfin, les sous-traitants doivent respecter la durée de conservation des données déterminée par le responsable du traitement.

G. – Le transfert des données

Le GT 29 réitère sa position (26) selon laquelle « *la constatation, l'exercice ou la défense d'un droit en justice* » (27) n'est pas une base légitime pour transférer tous les fichiers des salariés d'une filiale européenne vers la société mère située aux États-Unis, en vue d'un éventuel litige devant un tribunal américain. Néanmoins, le responsable du traitement peut se fonder sur cette exception lorsqu'il s'agit d'un transfert unique de toutes les informations pertinentes pour un litige particulier, à condition que ce transfert soit strictement limité quant aux personnes concernées et aux données transférées.
Hormis les exceptions énoncées à l'article 26 de la directive 95/46/CE, le transfert massif de données à caractère personnel vers un pays situé en dehors de l'Union européenne (28) qui n'a pas un niveau de protection adéquat (29) doit se fonder sur :
– l'adhésion aux règles de *Safe Harbor*, pour les données transférées vers les États-Unis ; ou
– des clauses contractuelles standards ; ou
– des règles internes d'entreprise (*Binding Corporate Rules*) préalablement approuvées par les autorités européennes de protection des données personnelles compétentes.
Enfin, le GT 29 reconnaît qu'un transfert de données qui est réalisé dans le cadre d'une requête adressée par un tribunal étranger, en application de la Convention de La Haye (30), est légitime.

(20) Données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, ainsi que les données relatives à la santé et à la vie sexuelle. (21) Voir article 8 de la directive 95/46/CE. (22) Voir article 10 de la directive 95/46/CE. (23) Pour plus d'informations sur cette question, voir l'avis 1/2006 du GT 29 relatif à l'application des règles européennes de protection des données aux dispositifs internes d'alerte professionnelle (« *whistleblowing* ») dans les domaines bancaire, de la comptabilité, du contrôle interne des comptes, de l'audit, de la lutte contre la corruption et les infractions financières, <http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2006_fr.htm>. (24) Voir articles 12 et 13 de la directive 95/46/CE. (25) Voir article 14 de la directive 95/46/CE. (26) Voir le document de travail n° 114 du GT 29 relatif à une interprétation commune des dispositions de l'article 26, paragraphe 1, de la directive 95/46/CE du 24 octobre 1995, adopté le 25 novembre 2005, <http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2005_en.htm>. (27) L'article 26(1)(d) de la directive 95/46/CE énonce qu'un transfert de données vers un État n'ayant pas un niveau de protection adéquat est possible lorsque « *le transfert est nécessaire ou rendu juridiquement obligatoire pour la sauvegarde d'un intérêt public important, ou pour la constatation, l'exercice ou la défense d'un droit en justice* ». (28) L'Union européenne s'entend ici des 27 pays membres de l'Union européenne ainsi que l'Islande, le Liechtenstein et la Norvège. Ces trois États sont membres de l'Association européenne de libre échange (AELE) et ont transposé la directive 65/46/CE dans leur droit national en application des obligations imposées à cet égard par l'accord sur l'Espace économique européen (EEE). (29) À ce jour, seuls l'Argentine, le Canada, l'Île de Guernesey, l'Île de Man, Jersey et la Suisse sont considérés par la Commission européenne comme assurant un niveau adéquat de protection des données à caractère personnel. Pour plus d'informations, voir <http://ec.europa.eu/justice_home/fsj/privacy/thridcountries/index_fr.htm>. (30) Convention sur l'obtention des preuves à l'étranger en matière civile ou commerciale, signée le 18 mars 1970, entrée en vigueur le 7 octobre 1972.

II. – LES LIMITES DU DOCUMENT DE TRAVAIL DU GT 29

Le document de travail du GT 29 n'a pas vocation à résoudre l'ensemble des conflits de droits relatifs aux p*re-trial discovery rules*. À juste titre, le GT 29 considère que la problématique du *e-discovery* dépasse son champ de compétence et que cette question doit être résolue conjointement par les gouvernements, éventuellement par le biais d'un traité ou d'une convention. Par ailleurs, le document de travail n'examine pas les règles spécifiques applicables en droit national (par exemple, le droit du travail, le respect de la vie privée, ou le secret des communications électroniques). Par conséquent, les entreprises concernées par une demande de *e-discovery* doivent s'assurer qu'elles respectent l'ensemble des dispositions législatives et réglementaires nationales ayant vocation à s'appliquer et pas seulement les dispositions relatives à la protection des données à caractère personnel. De même, le document de travail ne porte que sur les règles de procédure civile et exclut de son champ d'application les enquêtes internes ainsi que la production de documents dans le cadre d'une enquête criminelle ou d'une enquête initiée par une autorité administrative.

Le GT 29 rappelle également que la Convention de La Haye permet à un tribunal étranger d'obtenir la communication de documents par le biais d'une commission rogatoire et encourage son application dans les litiges internationaux. Néanmoins, il convient de souligner que la Convention de La Haye n'est pas la panacée. En effet, l'application de la Convention de La Haye se heurte à trois limites : premièrement, elle n'a pas été ratifiée par tous les États membres de l'Union européenne (par exemple, la Belgique) ; deuxièmement, parmi les États qui ont ratifié la Convention, certains ont émis une réserve qui leur permet de refuser d'exécuter une commission rogatoire (31) (par exemple, la France, l'Allemagne, l'Espagne et les Pays-Bas) ; enfin, s'agissant des États-Unis, la Cour suprême a jugé que le recours à la Convention de La Haye reste optionnel et n'est pas une procédure obligatoire d'obtention de preuves à l'étranger (32). Ainsi, si certains tribunaux américains semblent de plus en plus enclins à appliquer la Convention de La Haye lorsque les preuves se situent en Europe, la majorité des tribunaux américains hésite encore à appliquer cette convention, ou ignore son existence. Enfin, il est utile de rappeler que certaines lois nationales peuvent empêcher la communication de documents vers une juridiction étrangère (33).

> À juste titre, le GT 29 considère que la problématique du *e-discovery* dépasse son champ de compétence et que cette question doit être résolue conjointement par les gouvernements, éventuellement par le biais d'un traité ou d'une convention.

III. – LES SUITES DU CONFLIT DE DROITS EN MATIÈRE DE *E-DISCOVERY*

Le document de travail du GT 29 marque une première étape et doit être considéré comme une analyse initiale de la problématique de *e-discovery*. À ce titre, le document lance une consultation publique par laquelle toute partie intéressée (parties à un litige, tribunaux étrangers, sociétés, etc.) peut soumettre un avis au GT 29.

À défaut de répondre à toutes les questions, le document de travail du GT 29 a le mérite d'exister et de proposer des lignes directrices conformes au droit européen de protection des données à caractère personnel que les entreprises concernées peuvent appliquer à une demande de *e-discovery*. Les sociétés européennes veilleront ainsi à adapter leurs procédures et à mettre à jour leurs politiques internes (telles que la politique de protection des données personnelles, les notices d'informations ou la politique d'archivage des documents) en accord avec les recommandations du GT 29. De même, avant toute demande de *e-discovery*, les sociétés européennes s'assureront qu'elles traitent les données en Europe de manière légitime et proportionnée, et que le transfert des données vers un pays n'offrant pas un niveau de protection adéquat se fonde sur une base légale.

La question de savoir comment les cours et les tribunaux étrangers (notamment aux États-Unis) réagiront face à la position commune des autorités européennes reste difficile à prédire. Il est encore trop tôt pour dire si les juges anglo-saxons, dont certains connaissent peu ou mal les concepts européens de protection des données à caractère personnel, s'aligneront ou pas sur les recommandations du GT 29. N'oublions pas que les juges anglo-saxons conservent une indépendance et une autonomie dans leur pays et peuvent choisir d'ignorer les règles européennes de protection des données à caractère personnel s'ils les jugent trop fastidieuses à respecter. L'harmonie entre les règles de *e-discovery* et le droit européen de protection des données à caractère personnel reste donc un défi important pour les années à venir.

En définitive, ne serait-il pas envisageable que chaque autorité européenne de protection des données se saisisse séparément de ce dossier ? En effet, il serait peut-être opportun que ces autorités émettent un avis ou une recommandation précisant comment appliquer les règles de *e-discovery* conformément à leur droit national, tout en respectant le cadre commun défini par le GT 29 (34). Ceci aurait le mérite de compléter les lignes directrices du GT 29, et de garantir une plus grande sécurité juridique aux sociétés européennes. ◆

---

(31) Voir l'article 23 de la Convention de La Haye. **(32)** Voir *Société nationale industrielle aérospatiale v. United States District Court,* 482 U.S. 522, 544 n.28 (1987). **(33)** Pour plus d'informations sur les *blocking statutes*, voir note 2. **(34)** En Belgique, la Commission de la protection de la vie privée pourrait émettre une recommandation relative aux procédures de *e-discovery* semblable à celle qui a été rendue en matière de dispositifs d'alerte professionnelle. De même, en France, la CNIL pourrait préciser dans une délibération le régime applicable aux transferts de données réalisés dans le cadre d'un litige transnational.