RLDI 2465

À l'heure où la Commission européenne planche sur une réforme de la directive n° 95/46/CE relative à la protection des données personnelles et envisage d'introduire expressément le concept de « *Binding Corporate Rules* », il est opportun d'analyser cet instrument juridique et de comprendre les conditions de sa mise en œuvre.
Me Olivier Proust et Emmanuelle Bartoli se penchent sur le fonctionnement de ces règles d'entreprise contraignantes.

Les « *Binding Corporate Rules* » : une solution globale pour les transferts internationaux

Par Olivier PROUST
Avocat aux Barreaux de Paris et de Bruxelles
Cabinet Hunton & Williams

Et Emmanuelle BARTOLI
Attachée aux affaires européennes et internationales de la Cnil

INTRODUCTION

Le développement technologique et la globalisation de l'économie multiplient la collecte et la circulation des données personnelles à travers le monde. Des choix économiques ou stratégiques, tels que la délocalisation de certaines activités, l'attraction des marchés émergeants ou la réorganisation des systèmes d'information expliquent ce phénomène croissant auquel on assiste principalement au sein des sociétés multinationales. De nombreuses sociétés décident ainsi de centraliser toutes les données de leurs salariés dans une seule et même base de données située à l'étranger, le plus souvent hors de l'Union européenne. La mutualisation des systèmes d'information devient ainsi un mode de fonctionnement classique pour les entreprises.

Pourtant, en Europe, les transferts de données hors de l'Union européenne sont strictement encadrés par la directive n° 95/46/CE (1). En effet, les règles en matière de protection des données personnelles imposent aux entreprises de garantir un niveau de protection adéquat aux données personnelles qui sont transférées hors de l'Union européenne, c'est-à-dire un niveau de protection équivalant à celui qui existe au sein de l'Union européenne.

Pour se conformer à cette obligation, les entreprises disposent de différents instruments juridiques reconnus par la Commission européenne et par les autorités nationales de protection des données personnelles comme apportant un niveau de protection dit « *adéquat* » (2) (I). Parmi ces instruments, les règles d'entreprise contraignantes, ou « *Binding Corporate Rules* » (ci-après « BCR »), peuvent apporter une réponse juridique adaptée aux besoins et à la structure des sociétés multinationales (II). Une société qui se dote de BCR doit néanmoins obtenir la validation de ses BCR par les autorités nationales de protection des données personnelles (III).

I. – ANALYSE DES INSTRUMENTS JURIDIQUES PERMETTANT DE TRANSFÉRER LES DONNÉES PERSONNELLES EN DEHORS DE L'UNION EUROPÉENNE

Aux termes de la directive n° 95/46/CE, plusieurs instruments juridiques sont reconnus par la Commission européenne et les États membres comme apportant un niveau de protection adéquat. L'analyse des conditions et des instruments juridiques autorisant le transfert des données personnelles permet d'en apprécier les avantages et les inconvénients, et de comprendre l'intérêt que présentent les BCR pour les sociétés multinationales ou les grands groupes internationaux.

(1) Directive n° 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. (2) Un niveau de protection « *adéquat* » s'entend d'un régime de protection des données personnelles dans un pays tiers reconnu par la Commission européenne comme étant équivalent à celui apporté par la directive n° 95/46/CE.

A. – Le principe de l'interdiction de transférer des données personnelles vers des pays tiers

L'article 25 de la directive n° 95/46/CE pose un principe général selon lequel il est interdit de transférer les données à caractère personnel en dehors de l'Union européenne vers un pays tiers (3) qui n'a pas un niveau de protection adéquat des données personnelles (4). *A contrario*, un responsable de traitement présent sur le territoire de l'Union européenne peut librement transférer les données personnelles vers d'autres sociétés du groupe situées dans un État membre de l'Union européenne (5) ou de l'Espace économique européen (6). Tout autre transfert de données personnelles vers un pays tiers est en principe interdit à moins que la société exportatrice de données ne mette en œuvre un mécanisme juridique permettant de s'assurer du niveau de protection apporté aux données transférées. Plusieurs conditions et instruments juridiques (décrits ci-après) garantissent ce niveau de protection.

B. – Le statut de « *pays adéquat* »

La Commission européenne apprécie au cas par cas le caractère adéquat du niveau de protection offert par un pays tiers au regard de toutes les circonstances relatives à un transfert ou à une catégorie de transferts de données (7). En particulier, avant de rendre une décision d'adéquation à l'égard d'un pays tiers, la Commission prend en considération les règles de droit (8), générales ou sectorielles, en vigueur dans ce pays, ainsi que les règles professionnelles et les mesures de sécurité qui y sont applicables (9). Au 1er juillet 2011, seuls Andorre, l'Argentine, le Canada, Guernesey, l'île de Man, les îles Féroé, Jersey, Israël et la Suisse ont été reconnus par la Commission européenne comme ayant un niveau de protection adéquat.

Bien que la Commission européenne étudie à l'heure actuelle la candidature d'autres pays (par exemple, la Nouvelle-Zélande, l'Uruguay, la principauté de Monaco), la reconnaissance du niveau de protection adéquat de pays tiers se limite aujourd'hui à une poignée de pays. En particulier, les pays ou les régions vers lesquels sont transférées des données personnelles de manière massive et récurrente (par exemple, les États-Unis, la Chine, l'Inde, le Brésil, le Maroc, la Tunisie) ne sont pas reconnus pour l'heure comme disposant d'une protection adéquate. Ce constat démontre le manque d'harmonisation des législations en matière de protection des données et rappelle combien il est importa@nt pour les sociétés qui transfèrent régulièrement des données de s'assurer qu'elles garantissent un niveau de protection adéquat lorsqu'elles transfèrent des données à l'étranger.

> La Commission européenne apprécie au cas par cas le caractère adéquat du niveau de protection offert par un pays tiers au regard de toutes les circonstances relatives à un transfert ou à une catégorie de transferts de données.

C. – L'adhésion aux principes du « *Safe Harbor* »

En l'état actuel du droit, la législation américaine n'est pas reconnue comme adéquate. Néanmoins, en raison du nombre important de sociétés multinationales qui transfèrent et stockent leurs données personnelles aux États-Unis, un régime particulier a été négocié par les autorités européennes et américaines afin de ne pas entraver les échanges de données et le commerce entre l'Europe et les États-Unis. La Commission européenne et le Département du commerce américain (« *Federal Trade Commission* ») ont négocié et adopté une série de principes dits « *Safe Harbor* » inspirés de la directive n° 95/46/CE. Le « *Safe Harbor* » permet donc d'assurer une protection adéquate aux données transférées depuis l'Union européenne vers des entreprises établies aux États-Unis ayant adhéré à ces principes (10).

Cependant, le régime de « *Safe Harbor* » connaît certaines limites géographiques et juridiques. En effet, il ne s'applique qu'aux transferts réalisés vers des entreprises américaines ayant adhéré aux principes du « *Safe Harbor* » et ne peut pas s'appliquer à des transferts directs de données personnelles vers d'autres pays tiers. De même, les transferts de données vers des entreprises situées aux États-Unis mais qui n'ont pas adhéré aux principes du « *Safe Harbor* » doivent se fonder sur un autre instrument juridique (par exemple, les clauses contractuelles types). Par conséquent, si le « *Safe Harbor* » présente un intérêt pour les sociétés multinationales ayant centralisé leurs bases de données aux États-Unis, il peut se révéler juridiquement insuffisant lorsque ces données sont transférées vers de multiples pays tiers.

D. – Les clauses contractuelles types

L'article 26(2) de la directive n° 95/46/CE dispose qu'un responsable de traitement peut transférer les données personnelles vers un pays tiers n'ayant pas un niveau de protection adéquat s'il offre « *des garanties suffisantes au regard de la protection de la vie privée et des libertés et droits fondamentaux des personnes* » (11). Ces garanties peuvent

---

(3) Un pays tiers est défini comme tout pays non membre de l'Union européenne ou de l'Espace économique européen. Voir *Frequently Asked Questions relating to Transfers of Personal Data From the EU/EEA to Third Countries*, document publié par l'Unité data protection de la Direction générale justice au sein de la Commission européenne, <http://ec.europa.eu/justice/policies/privacy/international_transfers/index_en.htm>. **(4)** L'article 25 de la directive n° 95/46/CE a été transposé en droit interne sous l'article 68 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, lequel dispose : « *Le responsable d'un traitement ne peut transférer des données à caractère personnel vers un État n'appartenant pas à la Communauté européenne que si cet État assure un niveau de protection suffisant de la vie privée et des libertés et droits fondamentaux des personnes à l'égard du traitement dont ces données font l'objet ou peuvent faire l'objet.* » **(5)** Au 1er juillet 2011, les États membres de l'Union européenne sont : Allemagne, Autriche, Belgique, Bulgarie, Chypre, Danemark, Espagne, Estonie, Finlande, France, Grèce, Hongrie, Irlande, Italie, Lettonie, Lituanie, Luxembourg, Malte, Pays-Bas, Pologne, Portugal, République tchèque, Roumanie, Royaume-Uni, Slovaquie, Slovénie, Suède. **(6)** L'Espace économique européen est composé des États membres de l'Union européenne, ainsi que la Norvège, l'Islande, et le Liechtenstein. Ces trois pays ont transposé la directive n° 95/46/CE en droit interne. **(7)** Voir article 25(6) de la directive n° 95/46/CE. **(8)** La Commission vérifie notamment que le pays tiers offre un dispositif procédural de protection des données personnelles et apprécie, sur cette base, les différents mécanismes tant judiciaires qu'extrajudiciaires qui sont en vigueur dans ce pays. Voir le document de travail WP12, « *Transferts de données personnelles vers des pays tiers : application des articles 25 et 26 de la directive relative à la protection des données* », adopté par le Groupe de travail de l'article 29 le 24 juillet 1998, <http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/2005_en.htm>. **(9)** Voir article 25(2) de la directive n° 95/46/CE. **(10)** Voir Cnil, « *Transferts de données à caractère personnel vers des pays tiers à l'Union européenne* », <http://www.cnil.fr/vos-responsabilites/le-transfert-de-donnees-a-letranger/>. **(11)** L'article 26(2) de la directive n° 95/46/CE dispose : « *Sans préjudice du paragraphe 1, un État membre peut autoriser un transfert, ou un ensemble de transferts, de données à caractère personnel vers un pays tiers n'assurant pas un niveau de protection adéquat au sens de l'article 25, paragraphe 2, lorsque le responsable du traitement offre des garanties suffisantes au regard de la protection de la vie privée et des libertés et droits fondamentaux des personnes, ainsi qu'à l'égard de l'exercice des droits correspondants ; ces garanties peuvent notamment résulter de clauses contractuelles appropriées* ».

notamment résulter de clauses contractuelles appropriées telles qu'adoptées par la Commission européenne (12). Ces clauses permettent à un responsable de traitement établi dans l'Union européenne de transférer des données personnelles vers un autre responsable de traitement ou un sous-traitant qui est situé dans un pays tiers n'ayant pas le statut de pays adéquat.

En pratique, ces clauses types présentent un avantage pour les entreprises qui peuvent les reprendre *in extenso* en vue de garantir un niveau de protection adéquat aux données transférées. En revanche, un jeu de clauses contractuelles types doit être signé pour encadrer chaque transfert réalisé vers un pays tiers. On comprend alors aisément que le recours aux clauses contractuelles types peut se révéler administrativement lourd à gérer et réduit la visibilité du responsable de traitement quant aux différents transferts et à leur encadrement effectif. Ce constat est particulièrement vrai dans le contexte du *cloud computing* où la multiplication des prestataires et le nombre de serveurs auxquels ont recours certains prestataires augmentent le nombre de clauses à signer.

E. – Les dérogations légales

Enfin, l'article 26(1) de la directive n° 95/46/CE énumère plusieurs dérogations légales à l'interdiction de transférer des données vers des pays tiers (13). Ces exceptions s'interprètent de manière restrictive. En effet, l'article 26(1) a été conçu pour régler un nombre limité de cas dans lesquels une dérogation à l'exigence de protection adéquate a été considérée comme appropriée. De ce fait, les cas où une dérogation légale pourra s'appliquer sont limités et concernent des situations où le risque d'atteinte aux droits des personnes est faible (14).

Aux termes d'un avis rendu par le Groupe de l'article 29 (15) (ci-après « G29 »), les transferts « *répétés, massifs ou structurels* » vers des pays tiers ne pourront valablement être justifiés par une des exceptions énumérées à l'article 26(1) (16). Le G29 considère qu'une société multinationale devrait s'appuyer dans ce cas sur des « *garanties suffisantes* », telles que les clauses contractuelles types ou les règles d'entreprise contraignantes (BCR) (17). Ainsi, même si l'application des dérogations légales n'est pas totalement exclue, elle est largement limitée et n'a lieu de s'appliquer que dans des cas spécifiques et exceptionnels.

Bien que les différents instruments présentés ci-dessus garantissent tous un niveau de protection adéquat, ces instruments ne répondent pas toujours aux contraintes liées à la globalisation des échanges. Dans ce contexte, certaines entreprises préfèrent recourir à un instrument juridique qui offre une approche plus globale. Ainsi, les BCR apparaissent comme une alternative intéressante pour les sociétés multinationales car cet instrument juridique semble mieux adapté aux transferts massifs et récurrents au sein d'un groupe de sociétés.

II. – LE CHOIX DES BCR COMME ALTERNATIVE AUX ÉCHANGES DE DONNÉES AU SEIN D'UNE SOCIÉTÉ MULTINATIONALE

Conscient des limites des différents instruments juridiques permettant d'obtenir un niveau de protection adéquat, le G29 a jugé nécessaire d'autoriser les entreprises qui le souhaitent à encadrer les transferts réalisés au sein d'un groupe de sociétés par des règles internes contraignantes appelées « *Binding Corporate Rules* ».

Le G29 présente ainsi les BCR comme une alternative pouvant intéresser les sociétés multinationales puisqu'ils apportent des « garanties suffisantes » aux transferts de données personnelles au sein d'un groupe de sociétés.

A. – Un code de conduite pour encadrer les transferts intragroupes

Les BCR forment un ensemble de règles juridiques contraignantes, ou juridiquement exécutoires, qui s'appliquent aux transferts internationaux de données (18). À l'instar de ce qui existe dans d'autres domaines juridiques (par exemple, les politiques groupe en matière de protection de l'environnement, l'application de pratiques commerciales déontologiques, le respect des règles de concurrence sur le marché ou la lutte contre la corruption et le blanchiment d'argent), les BCR constituent un code de conduite (19) qui énonce la politique interne applicable aux transferts intragroupes de données personnelles (20). Ainsi, au lieu de mettre en œuvre différents instruments juridiques pour encadrer les transferts de données, les BCR permettent d'encadrer l'ensemble des transferts réalisés au sein du groupe grâce à un seul instrument juridique. Les BCR facilitent donc les transferts de données au sein d'un groupe tout en assurant un haut niveau de protection aux données personnelles quelle que soit l'entité du groupe vers laquelle elles sont transférées.

Les BCR permettent aussi d'accroître la confiance des personnes concernées à l'égard du responsable de traitement. En effet, une société peut faire valoir les BCR >

---

(12) Voir site de la Commission européenne : <http://ec.europa.eu/justice/policies/privacy/modelcontracts/index_en.htm>. **(13)** L'article 26(1) de la directive n° 95/46/CE dispose : « *Par dérogation à l'article 25 et sous réserve de dispositions contraires de leur droit national régissant des cas particuliers, les États membres prévoient qu'un transfert de données à caractère personnel vers un pays tiers n'assurant pas un niveau de protection adéquat au sens de l'article 25, paragraphe 2, peut être effectué, à condition que : a) la personne concernée ait indubitablement donné son consentement au transfert envisagé ou b) le transfert soit nécessaire à l'exécution d'un contrat entre la personne concernée et le responsable du traitement ou à l'exécution de mesures précontractuelles prises à la demande de la personne concernée ou c) le transfert soit nécessaire à la conclusion ou à l'exécution d'un contrat conclu ou à conclure, dans l'intérêt de la personne concernée, entre le responsable du traitement et un tiers ou d) le transfert soit 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 ou e) le transfert soit nécessaire à la sauvegarde de l'intérêt vital de la personne concernée ou f) le transfert intervienne au départ d'un registre public qui, en vertu de dispositions législatives ou réglementaires, est destiné à l'information du public et est ouvert à la consultation du public ou de toute personne justifiant d'un intérêt légitime, dans la mesure où les conditions légales pour la consultation sont remplies dans le cas particulier* ». **(14)** Voir WP114, « *Document de travail relatif à une interprétation commune des dispositions de l'article 26, paragraphe 1, de la directive n° 95/46/CE du 24 octobre 1995* », adopté le 25 novembre 2005, <http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/2005_en.htm>. **(15)** Le Groupe de travail de l'article 29 est l'organe communautaire composé d'un représentant de chaque autorité nationale de protection des données personnelles pour les 27 États membres de l'Union européenne et qui a pour mission d'examiner toute question portant sur la mise en œuvre des dispositions nationales prises en application de la directive n° 95/46/CE en vue de contribuer à leur mise en œuvre homogène. **(16)** Par exemple, le G29 considère que, dans une relation d'emploi, le consentement d'un salarié ne peut être donné librement en raison du lien de subordination entre l'employeur et le salarié. De surcroît, le consentement n'apparaît pas, à long terme, comme un fondement juridiquement viable, surtout lorsque le transfert est intrinsèquement lié au traitement lui-même. Ainsi, cette dérogation ne pourra pas s'appliquer dans l'hypothèse de la centralisation d'une base de données mondiale de ressources humaines dans un pays tiers qui nécessite des transferts répétés et permanents pour fonctionner. **(17)** Voirs *supra*, note 14. **(18)** Voir WP74 « *Document de travail : Transferts de données personnelles vers des pays tiers : Application de l'article 26(2) de la directive de l'UE relative à la protection des données aux règles d'entreprise contraignantes applicables aux transferts internationaux de données* », adopté, le 3 juin 2003, <http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/2003_en.htm>. **(19)** Par exemple, une politique interne dont l'application relève du siège social ou un code de conduite interne étayé par une convention interne à l'entreprise. **(20)** Voir *supra*, note 10.

comme argument de communication auprès de ses consommateurs, ses fournisseurs et ses clients, en démontrant qu'elle respecte les principes européens de protection des données personnelles. Les BCR apparaissent dès lors comme un instrument de communication, voire un argument de marketing, qui permet aux entreprises les ayant adoptés de se distinguer de leurs concurrents.

B. – Une politique globale pour la protection des données personnelles

Plus qu'un *corpus* de règles juridiques, les BCR permettent d'instaurer une véritable politique globale, une « *norme interne de référence* » (21), en matière de protection des données personnelles au sein du groupe. En effet, les BCR s'appliquent uniformément à l'ensemble du groupe, indépendamment du lieu d'implantation des filiales ou de la nationalité des personnes concernées par les traitements. Ils contribuent ainsi à uniformiser les pratiques et, ce faisant, à prévenir les risques inhérents aux traitements de données personnelles, en particulier au sein des sociétés membres du groupe établies dans des pays ne disposant pas d'une législation sur la protection des données personnelles. Les BCR permettent aussi d'introduire au sein de l'entreprise un ensemble de valeurs sociales autour de la protection et de la sécurité des données personnelles.

C. – Un ensemble de mesures concrètes visant à respecter les principes de protection des données personnelles

En pratique, le groupe qui adopte des BCR s'engage à prendre certaines mesures concrètes en vue de respecter les principes juridiques énoncés dans la directive n° 95/46/CE (22) (par exemple l'information des personnes concernées, la formation des salariés, la gestion des plaintes, la mise en place d'un programme d'audit, ou encore la création d'un réseau de responsables de la protection des données, etc.). Ces mesures sont mises en œuvre au cas par cas et peuvent varier selon le niveau de conformité de chaque société. Ainsi, nombre d'entreprises ont déjà mis en place ce type de mesures proactives et n'ont alors qu'à formaliser leurs engagements dans les BCR.

Dans le contexte de la révision de la directive n° 95/46/CE, le G29 a proposé d'introduire un principe de responsabilité (appelé « *accountability* » en anglais) aux termes duquel les responsables de traitement auront l'obligation de prendre des mesures proactives lors du traitement de données personnelles afin de démontrer aux autorités nationales de protection le respect des principes énoncés dans la directive (23). Si le concept d'*accountability* est introduit dans la révision de la directive n° 95/46/CE, les entreprises qui auront adopté et mis en œuvre des BCR seront déjà en mesure de démontrer leurs efforts de mise en conformité. De ce fait, les BCR apparaissent comme un véritable instrument d'*accountability*.

Plus qu'un *corpus* de règles juridiques, les BCR permettent d'instaurer une véritable politique globale, une « *norme interne de référence* », en matière de protection des données personnelles au sein du groupe.

D. – Un dispositif souple et sur mesure

Les BCR apportent plus de souplesse et de flexibilité que les clauses contractuelles types. Dans la pratique, l'utilisation des clauses contractuelles types peut se révéler très contraignante pour une société multinationale qui met en œuvre de nombreux transferts vers ses filiales (par exemple, lorsqu'elle transfère les mêmes données vers de multiples entités du groupe). Si les clauses contractuelles types apportent une certaine sécurité juridique au responsable de traitement (du fait qu'il s'agisse de clauses types adoptées par la Commission européenne), cette sécurité juridique s'acquiert aux dépens de toute flexibilité ou souplesse rédactionnelle. En cas de modification des clauses types, l'autorité nationale de contrôle se réserve le droit d'accepter ou non lesdites clauses. De plus, le champ d'application des clauses contractuelles types est strictement limité au transfert auquel elles s'appliquent. En cas de modification ultérieure du périmètre d'un transfert (par exemple, élargissement des catégories de données transférées, nouvelles finalités du transfert, ou multiplication des destinataires des données), ou lorsqu'une société met en œuvre un nouveau transfert, celle-ci doit soit modifier les clauses existantes, soit signer un nouveau jeu de clauses.

À l'inverse, les BCR permettent à une société de rédiger un corpus de règles juridiques qui répondent aux besoins, à la structure, à la culture et au mode de gouvernance de l'entreprise (24). La société définit elle-même le champ d'application géographique (par exemple, les filiales du groupe, les pays concernés) et matériel (par exemple, les types de traitement, les catégories des données, les catégories de personnes concernées) qui s'appliquent aux BCR. Elle peut également rédiger les BCR dans une langue et un style propres à la société, afin de les rendre clairs et compréhensibles pour l'ensemble de ses salariés, ses consommateurs et ses partenaires commerciaux. En définitive, les BCR se présentent comme un dispositif sur mesure que la société peut adapter à ses besoins. Les BCR présentent ainsi de nombreux avantages pour les sociétés multinationales, lesquelles doivent néanmoins faire valider leurs BCR par les autorités nationales de protection.

III. – LA PROCÉDURE DE VALIDATION DES BCR PAR LES AUTORITÉS NATIONALES DE PROTECTION

Il est de la compétence des autorités de protection de s'assurer que les engagements ainsi pris dans les BCR apportent un niveau de protection adéquat. Cette vérification s'effectue dans le cadre d'une procédure dite « de coopération »

(21) Voir Cnil, « *Transferts de données à caractère personnel vers des pays non membres de l'Union européenne* », juin 2008. **(22)** Ces principes sont notamment la légalité du traitement, la légitimité, la transparence, la proportionnalité et la sécurité. **(23)** Voir WP168, « *L'avenir de la protection de la vie privée : Contribution conjointe à la consultation de la Commission européenne sur le cadre juridique du droit fondamental à la protection des données à caractère personnel », adoptée le 1er décembre 2009,* <http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/2009_en.htm>. **(24)** Voir ICC, « *Report on binding corporate rules for international transfers of personal data* », préparé par ICC Task Force on Privacy and Protection of Personal Data, publié le 28 octobre 2004.

aux termes de laquelle l'ensemble des autorités reconnaît le caractère adéquat de l'instrument ainsi adopté par l'entreprise.

A. – La désignation d'une autorité chef de file

Les BCR doivent être validés par l'ensemble des autorités nationales de protection dans les pays de l'UE et de l'EEE depuis lesquels le responsable du traitement exporte des données. Afin d'éviter à la société déclarante d'avoir à répéter la procédure de validation auprès de chaque autorité, celle-ci désigne une autorité chef de file (ou autorité de coordination) en début de procédure chargée de coordonner et de recueillir la validation des BCR auprès de ses homologues européens. L'autorité chef de file est désignée selon des critères précis afin d'éviter que l'entreprise n'exerce un forum shopping auprès des autorités (par exemple, le lieu d'implantation du siège européen de la société, ou le lieu d'implantation de la société à laquelle ont été déléguées les responsabilités en matière de protection des données, ou encore le lieu d'implantation de la société qui est la mieux placée en termes de fonction, de gestion, et de charge administrative pour traiter la demande et mettre en œuvre les BCR au sein du groupe). Une fois que l'entreprise a identifié l'autorité chef de file, elle lui transmet un formulaire (25) comportant les arguments qui justifient cette désignation. Ce formulaire est ensuite transmis à l'ensemble des autorités de protection concernées qui ont 15 jours pour se prononcer sur sa désignation comme autorité chef de file. À l'expiration de ce délai, l'autorité concernée est officiellement désignée chef de file. De façon concomitante, l'entreprise a souvent commencé en amont à rédiger ses BCR et peut s'appuyer, pour ce faire, sur un ensemble de documents adoptés par le G29.

B. – Une « boîte à outils » pour aider les sociétés à préparer leurs BCR

En vue d'assister les sociétés dans la rédaction de leurs BCR, le G29 a adopté une série de documents (appelée communément « boîte à outils ») qui précisent les conditions et le contenu applicables aux BCR. À la suite d'un premier document de travail (WP74) (26) qui énonce les conditions générales applicables aux BCR, le G29 a adopté une grille de travail (WP153) (27) qui présente et explique les principes juridiques que la société s'engage à respecter. Ce document permet également aux autorités de se fonder sur un référentiel commun leur permettant d'évaluer le niveau de protection apporté par les BCR. Par ailleurs, le G29 a adopté un document de travail (WP154) (28) qui propose une structure possible des BCR et qui permet aussi à la société d'annexer des documents internes (par exemple, politique interne, directive, notice, guide, etc.) pour démontrer la mise en œuvre effective des BCR au sein du groupe. Enfin, soucieux d'apporter des réponses précises aux questions que peuvent se poser les entreprises (par exemple, sur le régime de responsabilité ou la clause de tiers bénéficiaire), le G29 a adopté un autre document sous la forme d'une foire aux questions (WP155) (29). L'ensemble de ces documents vise ainsi à faciliter la rédaction des BCR tout en garantissant une approche harmonisée au niveau européen. Les entreprises disposent ainsi de référentiels clairs reconnus comme valables par l'ensemble des autorités européennes.

Une fois que l'entreprise a rédigé ses BCR, elle les envoie à l'autorité chef de file qui les revoit et peut alors formuler des propositions de modification en vue d'aboutir à un document qui réponde aux attentes des autorités nationales de protection. La finalisation du texte des BCR se déroule généralement dans le cadre d'un dialogue entre l'entreprise et l'autorité de protection chef de file. Lorsque l'autorité chef de file juge les BCR satisfaisants, elle les communique à deux autres autorités de protection qui ont un mois pour les revoir et émettre d'éventuels commentaires. Une fois cette première étape achevée, l'autorité chef de file transmet alors le projet des BCR à l'ensemble des autorités de protection dans les pays concernés (c'est-à-dire les pays à partir desquels les données sont transférées). Commence alors une deuxième phase de validation dite « de coopération ».

C. – Une procédure de coopération accélérée grâce à la reconnaissance mutuelle

La procédure dite « *de coopération* » a pour but de s'assurer que toutes les autorités européennes de protection concernées reconnaissent les BCR comme apportant un niveau de protection adéquat et de valider cet instrument comme tel. Afin d'accélérer la validation des BCR par l'ensemble des autorités, le G29 a mis en place un système de reconnaissance mutuelle aux termes de laquelle la validation des BCR par l'autorité chef de file vaut approbation par l'ensemble des autorités ayant accepté ce mécanisme (30). Ainsi, les autorités en reconnaissance mutuelle accusent réception des BCR sans les revoir dans le détail, puisqu'elles se fondent sur la révision préalablement réalisée par l'autorité chef de file. Malgré l'intérêt que présente cette procédure, celle-ci n'est pas suivie pour le moment par toutes les autorités de protection européenne, bien que celles-ci soient de plus en plus nombreuses à comprendre l'intérêt que présente cette procédure et à l'adopter, grâce aux efforts du G29 (31). La procédure de reconnaissance mutuelle a également permis de réduire considérablement le délai de validation des BCR. Les autorités qui n'ont pas rejoint la procédure de reconnaissance mutuelle disposent de un mois pour revoir les BCR et pour adresser d'éventuels commentaires à l'autorité chef de file. Dans la pratique, ces autorités n'apportent généralement pas de modifications substantielles aux BCR et se fondent sur la validation initiale par l'autorité chef de file.

>

(25) Voir WP133, « *Standard Application for Approval of Binding Corporate Rules for the Transfer of Personal Data* », adopté le 10 janvier 2007, <http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/2007_en.htm>. **(26)** Voir *supra*, note 20. **(27)** Voir WP153, « *Document de travail établissant un tableau présentant les éléments et principes des règles d'entreprise contraignantes* », adopté le 24 juin 2008, <http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/2008_en.htm>. **(28)** Voir WP154, « *Document de travail établissant un cadre pour la structure des règles d'entreprise contraignantes* », adopté le 24 juin 2008, <http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/2008_en.htm>. **(29)** Voir WP155, « *Document de travail sur les questions fréquemment posées (FAQ) concernant les règles d'entreprise contraignantes* », adopté le 24 juin 2008, révisé en dernier lieu et adopté, le 8 avril 2009, <http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/2008_en.htm>. **(30)** Au 15 mai 2011, les pays ayant reconnu la procédure de reconnaissance mutuelle sont au nombre de 20 : l'Allemagne, l'Autriche, la Belgique, la Bulgarie, Chypre, l'Espagne, la France, la Grande-Bretagne, l'Irlande, l'Islande, l'Italie, la Lettonie, le Liechtenstein, le Luxembourg, Malte, la Norvège, les Pays-Bas, la République tchèque, la Slovaquie, et la Slovénie. **(31)** En particulier, la procédure de reconnaissance mutuelle ne fait pas perdre aux autorités nationales de protection leurs prérogatives puisque *in fine* ce sont elles qui autorisent formellement le transfert des données sur la base des BCR.

À l'issue de cette procédure, l'autorité chef de file renvoie les BCR à la société déclarante afin qu'elle puisse y apporter les modifications nécessaires à la validation finale. Lorsque la procédure de coopération est clôturée, les BCR sont formellement reconnus par l'ensemble des autorités de protection comme apportant un niveau de protection adéquat. L'entreprise peut alors se prévaloir de ses BCR pour transférer les données au sein du groupe (32).

CONCLUSION

Les avantages que présentent les BCR pour les sociétés multinationales attestent de l'intérêt croissant des entreprises pour cet instrument juridique. Plusieurs facteurs contribuent à cette évolution. Les entreprises semblent avoir pris conscience des risques inhérents aux transferts internationaux de données et démontrent une volonté plus forte d'encadrer ces transferts en leur apportant un niveau de protection adéquat. Par ailleurs, en comparaison avec d'autres instruments juridiques (tels que les clauses contractuelles types ou les dérogations légales), les BCR apportent une réponse globalisée aux problématiques de transferts intragroupes. La dimension pragmatique des BCR est particulièrement appréciée par les entreprises qui peuvent ainsi traduire concrètement leurs engagements dans un langage propre à la société. Les BCR permettent aussi aux entreprises de communiquer plus ouvertement auprès de leurs clients, fournisseurs et salariés sur les traitements mis en œuvre et la protection apportée aux données personnelles. Au-delà d'une contrainte légale, les BCR sont perçus aujourd'hui comme un argument concurrentiel. Enfin, longtemps critiquée en raison de sa longueur et de ses étapes laborieuses, la procédure de validation des BCR par les autorités nationales de protection a considérablement évolué vers plus de souplesse et de rapidité.

Dans ce contexte, le moment semble propice pour les entreprises de se lancer dans la préparation de leurs BCR. La révision de la directive n° 95/46/CE actuellement en cours pourrait conduire à une reconnaissance accrue des instruments dits d'« *accountability* ». Dans un proche avenir, il est vraisemblable que les entreprises auront le devoir, voire même l'obligation, de mettre en place des mesures proactives qui démontrent le respect et l'application des principes de protection des données énoncés dans la directive.

Enfin, certaines autorités nationales de protection ont annoncé leur volonté d'intensifier les contrôles relatifs aux transferts internationaux auprès des responsables de traitement (33). Dans ces conditions, les entreprises qui auront anticipé les risques inhérents à un contrôle (notamment le risque de sanction) en adoptant des BCR auront nécessairement une meilleure visibilité de leurs pratiques et seront donc mieux armées pour démontrer le respect des principes de protection des données personnelles auprès des autorités nationales de protection. ◆

---

(32) Il convient toutefois de préciser que la validation des BCR ne dispense pas le responsable du traitement des formalités préalables obligatoires auprès de chaque autorité nationale de protection dans le ou les pays où il traite des données et se prévaut des BCR pour transférer celles-ci en dehors de l'Union européenne. **(33)** Voir Cnil, « *Programme des contrôles 2011 : une ambition réaffirmée, des compétences élargies* », <http://www.cnil.fr/la-cnil/actu-cnil/article/article/programme-des-controles-2011-une-ambition-reaffirmee-des-competences-elargies/?tx_ttnews%5BbackPid%5D=2&cHash=91ae300acd>.