Le RGPD et les transferts internationaux de données à caractère personnel

De Terwangne, Cécile; Gayrel, Claire

Published in:
Le règlement général sur la protection des données (RGPD/GDPR)

Publication date:
2018

Document Version
le PDF de l'éditeur

TITRE 6
Le RGPD et les transferts internationaux de données à caractère personnel

Cécile DE TERWANGNE[1] et Claire GAYREL[2]

Introduction

1. Le développement des technologies de l'information et de la communication accompagné par la globalisation des marchés a, bien avant l'arrivée du règlement général sur la protection des données[3], suscité des questions quant à la réglementation des flux transfrontières de données à caractère personnel. À l'échelle mondiale, les négociations relative à l'Accord général sur le commerce des services de l'Organisation Mondiale du Commerce (AGCS, ou *GATS* en anglais pour *General Agreement on Trade in Services*) ont abouti à l'insertion d'une exception générale couvrant les mesures que les gouvernements pourraient juger nécessaires à « la protection de la vie privée des personnes pour ce qui est du traitement et de la dissémination de données personnelles ainsi qu'à la protection du caractère confidentiel des dossiers et comptes personnels »[4]. L'insertion de cette exception est généralement attribuée aux États européens, qui dans le même temps préparaient l'adoption de la directive 95/46/CE sur la protection des données et la libre circulation des données à caractère personnel

[1] Professeur à la Faculté de Droit de l'Université de Namur et directrice de recherches au CRIDS

[2] Claire Gayrel, précédemment chercheuse au CRIDS, est juriste auprès du Contrôleur européen de protection des données (CEPD). Les opinions exprimées dans cet article appartiennent exclusivement à son auteure et ne représentent en aucun cas celles du CEPD.

[3] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (ci-après RGPD).

[4] Organisation Mondiale du Commerce, Accord Général sur le commerce des Services signé à Marrakech le 15 avril 1994, article XIV c) ii). Voy. M.-V. PEREZ-ASINARI, « Is there any Room for Privacy and Data Protection within the WTO Rules ? », *Electronic Commerce Law Review*, 2002/9, pp. 249 et s. ; S. YAKOVLEVA et K. IRION, « The Best of Both Worlds ? Free Trade in Services and EU Law on Privacy and Data Protection », *EDPL*, 2016/2, pp. 191 et s.

dans l'Union[5]. Cette volonté politique des États européens de se doter d'un socle commun de protection des données, partiellement harmonisé dans un premier temps et presqu'uniformisé aujourd'hui, devait nécessairement s'accompagner de règles spécifiques en matière de transferts en dehors de l'Union afin de garantir que les données transférées dans des pays tiers restent protégées. Cette préoccupation de garantir la continuité du régime de protection au-delà des frontières est particulièrement vive actuellement face à la vie hyper-connectée et l'intensification toujours plus grande des échanges électroniques de données dans les contextes économiques, sociaux, politiques et privés qui conduisent à ce que ces données ne restent pas confinées à l'intérieur du territoire européen. Elles sont appelées à franchir les frontières et à sortir ainsi de leur zone de protection[6].

La problématique des flux transfrontières des données doit en conséquence être examinée sous deux angles : la situation des transferts intra-Union européenne (Chapitre 2) et le régime applicable aux transferts en dehors de l'Union européenne (Chapitre 3) auquel nous nous intéresserons plus spécifiquement dans le cadre de la présente contribution. Auparavant, il convient de préciser ce que recouvre la notion de « transfert » de données à caractère personnel (Chapitre 1).

CHAPITRE 1. La notion de transfert

2. Nulle trace d'une définition de la notion de transfert dans le RGPD, pas plus que dans la Directive qui l'a précédé. C'est particulièrement regrettable, d'autant que la notion avait été au cœur d'une affaire portée devant la Cour de justice qui n'avait pas apporté de réponse satisfaisante ni pleinement éclairante quant aux contours de cette notion dans le contexte d'Internet[7]. On aurait donc attendu du législateur européen qu'il prenne

[5] 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 de données à caractère personnel et à la libre circulation de ces données, *J.O.C.E.*, L 281 du 23 novembre 1995 (ci-après la « Directive »).

[6] La zone protégée couvre en fait les 28 États de l'Union européenne auxquels s'ajoutent les 3 États de l'Espace Économique Européen : la Norvège, le Lichtenstein et l'Islande.

[7] C.J.C.E., 6 novembre 2003, arrêt *Bodil Lindqvist*, C-101/01, §§ 56-70. La doctrine a relevé que le raisonnement suivi par la Cour dans cette affaire était trop lié aux circonstances spécifiques du cas pour permettre d'en tirer un éclairage général sur la notion de transfert de données. Voy. C. DE TERWANGNE, « Note d'observations sous C.J.C.E. du 6 novembre 2003 », *R.D.T.I.*, 2004/19, pp. 67-99 ; Ch. KUNER, *Transborder data Flows and Data Privacy Law,* Oxford University Press, 2013, pp. 12-13 ; M.V. PEREZ-ASINARI et Y. POULLET, « Privacy, Personal Data and the Safe Harbour

position en clarifiant la portée de la notion de transfert en présence de données mises à disposition sur des sites Web ouverts au monde.

3. Des éclaircissements ont toutefois été apportés à différents niveaux.

Ainsi, la Commission européenne a diffusé des FAQ dédiées aux transferts internationaux de données dans lesquelles elle a précisé que « The term "transfer of personal data" is often associated with the act of sending or transmitting personal data from one country to another,for instance by sending paper or electronic documents containing personal data by post or e-mail. Other situations also fall under this definition : all the cases where a controller takes action in order to make personal data available to a third party located in a third country »[8]. Le Contrôleur européen de la protection des données a, pour sa part, été dans le même sens lorsqu'il a précisé, dans son document d'orientation portant sur les flux transfrontières que « bien qu'il n'existe pas encore de définition formelle du 'transfert de données à caractère personnel', les responsables du traitement devraient considérer que cette expression renvoie normalement aux éléments suivants : la communication, la divulgation ou la mise à disposition par d'autres moyens de données à caractère personnel par un expéditeur relevant du règlement et conscient que le ou les destinataires y auront accès ou agissant dans cette intention »[9].

Le Rapport explicatif de la version modernisée de la Convention 108 du Conseil de l'Europe, adoptée le 18 mai 2018 par le Comité des Ministres du Conseil de l'Europe, précise de la même façon qu'« [u]n transfert transfrontière de données intervient lorsque des données à caractère personnel sont communiquées ou mises à disposition d'un destinataire relevant de la juridiction d'un autre État ou d'une autre organisation internationale »[10].

Decision », in *The Future of Transatlantic Economic Relations* (Andrews, Pollack, Schaffer (ed.)), Robert Schuman Center for Advanced Studies, 2005, p. 101 ; P. Van Den Bulck, « Transferts de données personnelles vers des pays tiers », *Bull. Ass. – De Verz.*, 2017, n° 22 Dossier *Data Protection L'impact du GDPR en assurance – De impact van de GDPR in de verzekering*, p. 213.

[8] Commission européenne, « Frequently Asked Questions Relating to Transfers of Personal Data from the Eu/Eea to Third Countries », mars 2009, p. 18 (ce document n'est plus disponible que dans une version archivée du site de la Commission européenne, à l'adresse http://collections.internetmemory.org/haeu/20171122154227/http://ec.europa.eu/justice/data-protection/international-transfers/files/international_transfers_faq.pdf).

[9] Contrôleur européen de la protection des données (EDPS), document d'orientation « Le transfert de données à caractère personnel à des pays tiers et à des organisations internationales par les institutions et organes de l'Union européenne », 14 juillet 2014, p. 7, https://edps.europa.eu/sites/edp/files/publication/14-07-14_transfer_third_countries_en.pdf (le règlement évoqué par l'EDPS dans cette définition est le règlement (CE) 45/2001 mais la définition donnée peut être transposée dans le cadre du RGPD).

[10] Protocole d'amendement à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE n° 108), Rapport explicatif, adopté

La directive 2016/681 relative à la protection des données à caractère personnel en matière de police et justice[11] votée le même jour que le RGPD évoque, quant à elle, les échanges de données à caractère personnel entre autorités compétentes, et vise par-là à s'appliquer aux « données à caractère personnel qui sont transmises ou mises à disposition entre les États membres »[12]. Ainsi, même si elle évoque les échanges plutôt que les transferts de données, cette norme européenne indique, elle aussi, la voie d'une perception non plus métaphorique de données qui seraient véritablement en mouvement avec blocage ou non aux frontières, mais opérationnelle, impliquant la reproduction ou l'accessibilité des données depuis des zones hors de la juridiction des États membres de l'UE[13].

Au demeurant, il n'est pas évident d'un point de vue technique d'établir une distinction nette entre l'accès et la transmission délibérée. Dans bien des cas, l'accès à des informations peut prendre la forme d'une consultation mais également d'un transfert, Ainsi, lorsque l'accès à un registre se réalise par une interrogation à distance, en ligne, ce qui pourrait à première vue être assimilé à une consultation à distance correspond techniquement à un envoi de données. La Cour de justice a d'ailleurs elle-même fait cette observation technique puisqu'elle énonce que pour qu'un internaute puisse accéder à des données mises à disposition sur un site internet, il faut que, suite à la démarche de cet internaute, les données en question arrivent sur son ordinateur, en provenance de l'hébergeur du site[14]. Ce n'est pas l'internaute qui se rend virtuellement sur le site souhaité, ce sont des copies du site qui sont envoyées sur son ordinateur[15].

Il convient enfin de mettre en exergue la *ratio legis* du régime spécifique mis en place concernant les flux transfrontières de données. Ce que les auteurs de la directive ont voulu, c'est empêcher qu'une fois hors de la forteresse-Europe, les données connaissent un sort peu enviable car ne bénéficiant plus d'aucune protection. Ils ont donc instauré un régime

---

par le Comité des Ministres du Conseil de l'Europe, à Elseneur, Danemark, le 18 mai 2018, § 101, disponible à https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=090000168089ff4b.

[11] Directive 2016/680/UE du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil.

[12] Considérant n° 7 de la directive 2016/681.

[13] G. Gonzalez Fuster, « Un-mapping Personal Data Transfers », *European Data Protection Law Review*, 2016, (2) 2(2), pp. 160-168.

[14] C.J.C.E., 6 novembre 2003, arrêt *Bodil Lindqvist*, C-101/01, pts 59 à 61.

[15] C. de Terwangne, « Affaire Lindqvist ou quand la Cour de Justice des Communautés européennes prend position en matière de protection des données personnelles », note sous C.J.C.E., 6 novembre 2003, arrêt *Bodil Lindqvist*, C-101/01, *R.D.T.I.*, 2004/19, p. 91.

n'admettant que les données sortent de l'Union européenne que pour aller vers les zones sûres. Il serait paradoxal de vouloir qu'en dehors de l'Europe les données « européennes » jouissent d'une certaine protection et de mettre en place un système qui ne protègerait que les données que l'on fait sortir et non les données que l'on laisse sortir. En réponse au débat sur la distinction entre transfert délibéré et accessibilité des données, au-delà des considérations déjà émises plus haut, il s'indique de conclure qu'il n'est pas rationnel de distinguer faire sortir et laisser sortir[16].

En résumé, la notion de transfert couvre toute transmission, copie ou déplacement de données d'un responsable de traitement situé dans l'Union vers un destinataire établi dans un État tiers, mais également toute publication ou mise à disposition consciente de données à caractère personnel[17]. « *In this sense, (free) 'data flows' are basically unrestricted operations of data multiplication under a single (European) jurisdiction, and 'data transfers' are fundamentally acts whereby data are made available for the reproduction into another jurisdiction* »[18].

Par ailleurs, le RGPD a vocation à s'appliquer tant à des transferts entre responsables de traitement qu'entre un responsable de traitement et un sous-traitant ou entre sous-traitants.

À titre d'exemples, la centralisation au sein d'un même groupe de données relatives à la facturation des clients, à la gestion des ressources humaines d'une multinationale, ou bien le transfert à un prestataire aux fins de saisie informatique de dossiers manuels ou à un centre d'appel étranger, ou enfin l'hébergement et l'exploitation de plateformes informatiques constituent des transferts internationaux de données. L'EDPS a pour sa part illustré la notion par les exemples suivants : « l'envoi « *push* » de données à partir de la base de données d'un responsable du traitement des données de l'Union à un destinataires d'un pays tiers ; l'octroi de l'accès à la base de données d'un responsable du traitement des données de l'Union (« *pull* ») à un destinataire d'un pays tiers ; la publication de

[16] C. de Terwangne, « Affaire Lindqvist ou quand la Cour de Justice des Communautés européennes prend position en matière de protection des données personnelles », *op. cit.*, p. 93.

[17] Voy. égal. les développements très fouillés dans G. Gonzalez Fuster, « Un-mapping Personal Data Transfers », *op. cit.*, pp. 160-168. L'auteur relève un ensemble de textes en lien avec les transferts de données à caractère personnel. Voy. aussi la très pertinente proposition de Christopher Kuner de ne pas s'attarder à vérifier si les données sont « passivement » rendues accessibles ou « activement » transmises, mais d'appliquer le régime des flux transfrontières dès que des données à caractère personnel sont traitées hors du pays où elles ont été collectées initialement (Ch. Kuner, *Transborder data Flows and Data Privacy Law*, *op. cit.*, pp. 174-175).

[18] G. Gonzalez Fuster, « Un-mapping Personal Data Transfers », *op. cit.*, p. 168.

données à caractère personnel sur l'internet par un responsable du traitement des données de l'Union ; [...] »[19].

CHAPITRE 2. La libéralisation des transferts intra-Union européenne

SECTION 1. – Les transferts couverts par le RGPD et les autres

4. Il faut distinguer essentiellement deux sous-catégories de transferts au sein de l'Union européenne. Premièrement, il y a les transferts de données à caractère personnel dont le traitement entre dans le champ d'application du RGPD. Ensuite, il y a les transferts qui ont lieu dans le cadre de la coopération entre autorités compétentes des États membres à des fins de prévention, de détection et de poursuite des infractions pénales, qui sont, quant à eux, encadrés par la directive (UE) 2016/680 du 27 avril 2016 relative à la protection des données en matière pénale[20]. Le propos de ce chapitre sera centré exclusivement sur les transferts de données à caractère personnel couverts par le RGPD et non sur ceux liés à la coopération en matière pénale, pas plus que sur les transferts de données par les autorités nationales compétentes à

[19] Contrôleur européen de la protection des données (EDPS), document d'orientation « Le transfert de données à caractère personnel à des pays tiers et à des organisations internationales par les institutions et organes de l'Union européenne », 14 juillet 2014, p. 8, https://edps.europa.eu/sites/edp/files/publication/14-07-14_transfer_third_countries_en.pdf

[20] Directive 2016/680/UE du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil. Voy. égal. le Umbrella Agreement UE-USA organisant l'échange de données dans le cadre de la prévention et de la détection des infractions pénales, F. Boehm, « Assessing the New Instruments in EU-Us Data Protection Law for Law Enforcement and Surveilance Purposes », *EDPL*, 2016/2, pp. 178 et s. ; les décisions adoptées pour encadrer certains échanges de données : les transferts des données des dossiers passagers (données PNR) (vers les États-Unis : décision du Conseil 2012/472/UE du 26 avril 2012 ; vers l'Australie : Council Decision 2008/651/CFSP/JHA of 30 June 2008 ; et vers le Canada : le projet d'accord du 5 décembre 2013 soumis pour approbation au Parlement européen a fait l'objet d'une opinion de la Cour de justice, voy. C.J.U.E., 26 juillet 2017, opinion 1/15, C. Kuner, « Data Protection, Data Transfers, and International Agreements : the CJEU's Opinion 1/15 », 26 July 2017, *Verfassungsblog*, https://verfassungsblog.de/data-protection-data-transfers-and-international-agreements-the-cjeus-opinion-115) et les transferts de données de messagerie financière de l'Union européenne aux États-Unis aux fins du programme de surveillance du financement du terrorisme - Data and Terrorist Finance Tracking Programme (TFTP) (décision du Conseil 2010/412 du 13 juillet 2010).

des systèmes d'information européens encadrés par des instruments spécifiques comme la Convention Europol, les différentes décisions portant création du Système d'Information Schengen, du Système d'Information des Visas, d'Eurodac ou encore du Système d'Information Douanier[21].

SECTION 2. – Le principe de la liberté de circulation des données à caractère personnel

5. Le principe de la liberté de circulation des données à caractère personnel au sein de l'Union, et plus largement dans l'Espace économique européen (EEE)[22], est l'objectif fondamental de l'adoption du RGPD et, avant lui, de la directive 95/46/CE[23]. Le RGPD vise expressément à l'uniformisation des règles et du niveau de protection des données entre les États membres de l'Union européenne aux fins précisément de libéraliser les flux de données dans l'Union conformément à l'objectif général d'accomplissement du marché intérieur[24]. « Pour que le marché intérieur fonctionne correctement, il est nécessaire que la libre circulation des données à caractère personnel au sein de l'Union ne soit ni limitée ni interdite

[21] Pour un examen exhaustif des instruments prévoyant et organisant l'échange de données à caractère personnel entre États Membres dans le cadre de l'Espace de Liberté, Sécurité et Justice avant l'adoption du RGPD et de la directive 2016/680, voy. F. BOEHM, *Information Sharing and Data Protection in the Area of Freedom, Security, and Justice*, Springer, 2012.

[22] À propos de l'incorporation du RGPD dans l'EEE, voy. la déclaration de l'Association européenne de Libre Echange (AELE/EFTA) : « A lot of work has been undertaken in recent months to ensure its timely incorporation into the EEA Agreement. A Joint Committee Decision (JCD) incorporating the GDPR is expected to be adopted by the EEA Joint Committee on 6 July 2018 and enter into force in the EEA EFTA States in mid-July 2018. Until then the Data Protection Directive 95/46/EC remains applicable in the EEA Agreement thus ensuring that data can continue to flow freely between the EEA EFTA States and the EU Member States », disponible sur le site de l'AELE http://www.efta.int/About-EFTA/news/Incorporation-General-Data-Protection-Regulation-GDPR-EEA-Agreement-and-continued-application-Directive-9546EC-508856.

[23] B. HAVELANGE et A.-C. LACOSTE, « Les flux transfrontaliers de données à caractère personnel en droit européen », *J.D.E.*, 2001, pp. 241 et s.

[24] Voy. not. considérants n^{os} 3 à 10 de la directive 95/46/CE, dont le considérant n° 3 : « considérant que l'établissement et le fonctionnement du marché intérieur dans lequel, conformément à l'article 7 A du traité, la libre circulation des marchandises, des personnes, des services et des capitaux est assurée, nécessitent non seulement que des données à caractère personnel puissent circuler librement d'un État membre à l'autre, mais également que les droits fondamentaux des personnes soient sauvegardés ». Et, vingt-et-un an plus tard, le considérant n° 5 du RGPD : « L'intégration économique et sociale résultant du fonctionnement du marché intérieur a conduit à une augmentation substantielle des flux transfrontaliers de données à caractère personnel. Les échanges de données à caractère personnel entre acteurs publics et privés, y compris les personnes physiques, les associations et les entreprises, se sont intensifiés dans l'ensemble de

pour des motifs liés à la protection des personnes physiques à l'égard du traitement des données à caractère personnel »[25]. Le choix d'un instrument juridique tel un règlement européen pour assurer la protection des données s'explique par cet objectif : « Afin d'assurer un niveau cohérent et élevé de protection des personnes physiques *et de lever les obstacles aux flux de données à caractère personnel au sein de l'Union*, le niveau de protection des droits et des libertés des personnes physiques à l'égard du traitement de ces données devrait être équivalent dans tous les États membres »[26].

L'article premier du RGPD proclame ce double objectif de protection des personnes physiques à l'égard du traitement de leurs données à caractère personnel et de libre circulation des données[27]. Les règles contenues dans le RGPD servent toutes ce double objectif, contrairement à ce que pourrait laisser croire la formulation du paragraphe premier de cette disposition selon laquelle le RGPD établit « des règles relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et des règles relatives à la libre circulation de ces données ». Il n'y a pas deux types de règles dans le RGPD, au service de deux objectifs distincts, mais un ensemble de règles exprimant l'équilibre trouvé pour réaliser au mieux les deux objectifs.

La protection des individus étant garantie si l'on respecte l'ensemble des règles contenues dans le RGPD, il n'est plus question de limiter ni d'interdire la circulation des données à caractère personnel au sein de l'Union pour des motifs liés à la protection des personnes physiques à l'égard du traitement des données à caractère personnel[28].

SECTION 3. – Condition de licéité des transferts intra-UE : le respect du chapitre II du RGPD

6. En revanche, il faut souligner que les transferts de données à caractère personnel constituent aussi des traitements ou sont des opérations faisant

l'Union. Le droit de l'Union appelle les autorités nationales des États membres à coopérer et à échanger des données à caractère personnel, afin d'être en mesure de remplir leurs missions ou d'accomplir des tâches pour le compte d'une autorité d'un autre État membre ».

[25] Considérant n° 13 du RGPD.

[26] Considérant n° 10 du RGPD (nos italiques). Égal. considérant n° 13 : « Afin d'assurer un niveau cohérent de protection des personnes physiques dans l'ensemble de l'Union, et d'éviter que des divergences n'entravent la libre circulation des données à caractère personnel au sein du marché intérieur, un règlement est nécessaire […] ».

[27] Art. 1er, § 1er, du RGPD.

[28] Art. 1er, § 3, du RGPD.

partie d'un traitement, au sens du RGPD et doivent donc être conformes à tous les principes contenus au chapitre II du RGPD, et notamment à l'article 5 : principes de licéité, loyauté et transparence ; limitation des finalités ; minimisation des données ; exactitude ; limitation de la conservation ; et intégrité et confidentialité[29].

Il y a donc une condition à cette libre circulation : on ne peut transférer des données à caractère personnel que si cette opération est admissible aux yeux du RGPD, c'est-à-dire principalement si ce transfert s'impose pour réaliser la finalité annoncée du traitement ou s'il est compatible avec cette finalité, ou encore s'il découle d'une obligation légale[30]. Sinon, il faut obtenir le consentement de la personne concernée pour pouvoir effectuer le transfert[31]. À titre d'exemple de transfert compatible avec la finalité du traitement des données, un cabinet d'avocats implanté à Bruxelles peut ainsi envoyer à la succursale d'Amsterdam la liste des clients qui se sont présentés à lui afin de vérifier si le bureau d'Amsterdam n'a pas ces clients comme adversaires dans d'autres affaires et d'éviter dès lors d'éventuelles incompatibilités. Par ailleurs, seules les données pertinentes au regard de la finalité poursuivie, et limitées à ce qui est nécessaire, peuvent faire l'objet du transfert.

CHAPITRE 3. Les transferts en dehors de l'Union européenne

7. Les transferts de données en dehors de l'Union européenne sont les transferts qui nous intéressent plus spécifiquement dans le cadre de la présente contribution. Ils sont visés au chapitre V du RGPD. Il s'agit donc des transferts de données à caractère personnel au départ d'un État membre de l'Union à destination d'un pays tiers à l'EEE, ou à destination d'une organisation internationale[32].

[29] Pour une présentation et analyse de ces principes, voy. la contribution de C. DE TERWANGNE dans le présent ouvrage : « Les principes relatifs au traitement des données à caractère personnel et à sa licéité ».

[30] Art. 5, § 1, b), et art. 6, § 4, du RGPD.

[31] Art. 6, § 4, du RGPD.

[32] L'article 4.26 du RGPD stipule que par « organisation internationale » il faut entendre « une organisation internationale et les organismes de droit public international qui en relèvent, ou tout autre organisme qui est créé par un accord entre deux pays ou plus, ou en vertu d'un tel accord ».

Ces transferts dits « internationaux » sont soumis à certaines conditions. Ces conditions n'ont pas fondamentalement changé par rapport à ce qui régissait les transferts hors UE sous l'empire de la directive 95/46. Toutefois, les enseignements tirés de la jurisprudence de la Cour de justice de l'Union européenne – notamment de son retentissant arrêt *Schrems*[33] – et des avis du Groupe de l'article 29[34] se reflètent désormais dans le texte du RGPD. Ainsi, par exemple, les critères à prendre en considération pour déterminer si un pays tiers ou une organisation internationale offre une protection adéquate ont été clarifiés et la palette des instruments juridiques permettant d'apporter des garanties appropriées pour encadrer les flux de données est élargie.

Dans les pages qui suivent, nous nous attacherons aux dispositions du RGPD[35] qui visent à garantir que les données à caractère personnel qui sont transférées continuent à bénéficier d'une protection satisfaisante après leur transfert vers le pays de destination : soit le transfert a lieu vers un pays tiers destinataire offrant une protection adéquate (Section 1), soit le transfert est encadré par des garanties appropriées (Section 2). Puis nous verrons les exceptions prévues par le RGPD à ces deux situations, permettant de transférer, dans des circonstances particulières, des données vers un pays n'offrant pas un niveau adéquat de protection, et en dehors de garanties suffisantes (Section 3).

8. Ces trois possibilités de transferts, composant le régime juridique des flux transfrontières, sont commentées dans l'ordre dans lequel elles sont présentées dans le RGPD, qui correspond à l'ordre d'utilisation qui avait été recommandé par le Groupe de l'article 29. Ainsi, la meilleure pratique à adopter pour un responsable de traitement envisageant de transférer des données en dehors de l'Union européenne consiste en premier lieu à examiner si le pays tiers garantit un niveau adéquat de protection des données. Dans le cas contraire, le responsable de traitement devrait en second lieu envisager d'encadrer les transferts de garanties suffisantes, au moyen notamment de clauses contractuelles appropriées ou de règles d'entreprise contraignantes. Ce n'est que dans les cas où cela s'avère impossible que le responsable de traitement devrait envisager en dernier lieu le recours à l'une des dérogations prévues par le RGPD[36].

---

[33] C.J.U.E. (GC), arrêt du 6 octobre 2015, *Maximillian Schrems c. Data Protection Commissioner*, C-362/14, EU :C :2015 :650.

[34] Il s'agit du Groupe européen des autorités de protection des données établi à l'article 29 de la directive 95/46/CE.

[35] Soit les art. 44 à 49 du RGPD.

[36] Groupe 29, Document de travail relatif à une interprétation commune des dispositions de l'article 26, paragraphe 1, de la directive 95/46/CE adopté par le Groupe le 25 novembre

9. Enfin, on relèvera que le RGPD apporte aussi la nouveauté que si, comme auparavant, le responsable du traitement doit respecter les règles en matière de flux transfrontières de données, les sous-traitants sont désormais également expressément tenus au respect de ces règles[37].

SECTION 1. – Les transferts vers une destination offrant une protection adéquate (art. 45 du RGPD)

10. Ainsi qu'on l'a dit, le RGPD, à l'instar de la directive 95/46[38], accepte les transferts de données à caractère personnel qui s'effectuent en direction de pays (ou d'organisations internationales[39]) qui assurent « un niveau de protection adéquat »[40].

Il est à noter que ces textes ne spécifient pas expressément sur quoi doit porter cette protection. La directive évoquait les cas où la Commission peut constater qu'un pays tiers « assure un niveau de protection adéquat, en raison de sa législation interne ou de ses engagements internationaux, […] en vue de la *protection de la vie privée et des libertés et droits fondamentaux des personnes* »[41]. On retrouve cet objectif de protection des droits fondamentaux des personnes concernées dans le RGPD[42]. Mais les deux textes évoquent aussi la « protection des personnes »[43] et le règlement ajoute que la Commission peut décider qu'un pays tiers, un secteur déterminé dans un pays tiers, ou une organisation internationale offre un niveau adéquat de protection « des données »[44]. La protection adéquate qui doit être assurée au-delà des frontières européennes est donc celle qui est accordée aux personnes concernées, à leurs droits fondamentaux ou à leurs données à caractère personnel.

2005, WP 114, pt 1.3, p. 10.

[37] Art. 44 du RGPD.

[38] Art. 25, § 1, de la directive 95/46.

[39] Les organisations internationales ne sont visées comme destinataires de données que par le RGPD.

[40] Art. 45, § 1er, du RGPD.

[41] Art. 25, § 6, de la directive 95/46 (c'est nous qui soulignons).

[42] Considérant n° 102, *in fine*, du RGPD : « Les États membres peuvent conclure des accords internationaux impliquant le transfert de données à caractère personnel vers des pays tiers ou à des organisations internationales dans la mesure où ces accords n'affectent pas le présent règlement ou toute autre disposition du droit de l'Union et prévoient un niveau approprié de protection des droits fondamentaux des personnes concernées ».

[43] Considérant n° 56 de la directive 95/46 ; considérant n° 101 du RGPD.

[44] Considérant n° 103 du RGPD.

Un tel transfert de données vers un pays ou une organisation qui ont été reconnus comme garantissant une protection adéquate ne nécessite pas d'autorisation spécifique[45].

Le paragraphe 3 ci-dessous s'attache à expliquer les critères à prendre en compte pour déboucher sur une décision d'adéquation de la protection offerte au-delà des frontières de l'EEE, mais auparavant, il convient de préciser la portée que peut avoir une décision d'adéquation (§ 1) et d'identifier l'auteur d'une telle décision (§ 2). Nous poursuivrons nos développements en évoquant ce qu'il advient après la décision d'adéquation (§ 4) et terminerons en nous penchant sur ce qu'il reste de pouvoir aux autorités de contrôle une fois une décision d'adéquation adoptée par la Commission (§ 5).

§ 1. Portée de la décision d'adéquation

a) Adéquation de la protection offerte par un pays ou une organisation internationale

11. Aux termes du paragraphe 1er de l'article 45 du RGPD, l'évaluation de l'adéquation de la protection offerte peut porter non seulement sur la situation d'un pays tiers[46] mais aussi sur celle d'organisations internationales[47] (telles le CICR, par exemple, situé à Genève, ou l'AMA – l'Agence Mondiale Anti-dopage, située à Montréal et vers laquelle de nombreuses données sensibles sur la santé des sportifs de haut niveau sont systématiquement envoyées en provenance de l'Union européenne[48]). C'est une nouveauté du RGPD dès lors que la Directive n'envisageait que l'adéquation de pays tiers.

b) Adéquation d'une protection nationale, régionale ou sectorielle

12. Par ailleurs, le RGPD précise que les constats d'adéquation peuvent être restreints à un territoire[49] ou à un ou plusieurs secteurs déterminés dans le pays tiers. Ce type d'adéquation partielle a en fait déjà été reconnu

[45] Art. 45, § 1er, du RGPD.

[46] Pour rappel, il s'agit de pays tiers à l'Espace Économique Européen.

[47] Pour l'application du RGPD, et notamment des dispositions concernant les flux transfrontières de données, aux organisations internationales, voy. Ch. KUNER, « International Organizations and the EU General Data Protection Regulation », *University of Cambridge Faculty of Law Research Paper*, No. 20/2018, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3050675.

[48] Voy. J. MONT, « Protection de la vie privée du sportif d'élite & whereabouts : deux notions inconciliables ? », *R.D.T.I.*, 2016, n° 61, pp. 21-41.

[49] L'attention de la Commission a ainsi été attirée sur la situation du Québec qui est actuellement toujours l'objet d'analyse.

pour le Canada où seule la protection mise en place pour le secteur privé a été estimée adéquate, en raison essentiellement de l'existence d'une législation de protection spécifique à ce secteur[50]. Une décision d'adéquation portant sur un secteur d'activité particulier, comme le secteur financier ou le secteur des assurances ou encore le secteur d'activité de la sous-traitance des traitements de données, peut ainsi être accordée en tenant compte de réglementations et de pratiques spécifiques au secteur en question qui assurent une protection adéquate aux données à caractère personnel transférées.

§ 2. Auteur et forme de la décision d'adéquation

13. La Commission européenne est désormais seule aux commandes d'une décision d'adéquation alors que sous le régime de la Directive, la prérogative d'autoriser, en cas d'adéquation du niveau de protection, ou d'interdire, en cas d'inadéquation du niveau de protection, les transferts de données vers des pays tiers appartenait également aux États membres[51].

14. La décision d'adéquation prend la forme d'un acte d'exécution qui doit être adopté en conformité avec la procédure d'examen prévue à l'article 5 du règlement 182/2011[52]. Ainsi, avant de prendre sa décision, la Commission doit recevoir l'approbation d'un comité composé des représentants des États membres de l'UE. Le Comité européen de la protection des données (CEPD) est précédemment appelé à donner son avis sur l'évaluation du caractère adéquat du niveau de protection assuré par un pays ou une organisation visés par un projet de décision d'adéquation[53].

15. À ce jour, la Commission européenne a adopté des décisions d'adéquation[54] concernant : Andorre, l'Argentine, le Canada, la Suisse, les Iles Féroé, Guernesey, l'Ile de Man, Jersey, Israël, la Nouvelle-Zélande et l'Uruguay, de même que pour les entreprises américaines ayant souscrit aux

---

[50] Décision 2002/2/CE de la Commission du 20 décembre 2001 constatant, conformément à la directive 95/46/CE du Parlement européen et du Conseil, le niveau de protection adéquat des données à caractère personnel assuré par la loi canadienne sur la protection des renseignements personnels et les documents électroniques, *J.O.C.E.*, L 2 du 4 janvier 2002.

[51] C. Gayrel, « Le régime des transferts internationaux de données à caractère personne », in C. de Terwangne (éd.), *Vie privée et données à caractère personnel*, Bruxelles, Politeia, 2014.

[52] Règlement 182/2011 établissant les règles et principes généraux relatifs aux modalités de contrôle par les États membres de l'exercice des compétences d'exécution par la Commission, *J.O.U.E.*, L 55/13.

[53] Art. 70, § 1er, s), du RGPD.

[54] Voy. le site de la Commission dédié aux flux transfrontières de données, https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu_en.

principes du « Bouclier de protection des données » ou « *Privacy Shield* »[55], venu remplacer la « Sphère de sécurité » (« *Safe Harbor* ») après l'invalidation de cette dernière par la Cour de justice dans son arrêt *Schrems*[56]. Ce qui signifie, comme on l'a dit, que pour ces destinations, et dans les limites du champ d'application du RGPD[57] et de la décision de la Commission[58], les transferts sont par principe autorisés et ne requièrent pas de formalités particulières pour le responsable de traitement ou le sous-traitant établi dans l'Union[59]. « *In others words, transfers to the country in question will be assimilated to intra-EU transmissions of data* »[60].

Le RGPD a expressément signalé que ces décisions prises sous le régime de la Directive demeurent en vigueur jusqu'à leur éventuelle révision ou abrogation[61].

---

[55] L'accord du Privacy Shield a fait l'objet de deux recours en annulation, l'un initié par Digital Rights Ireland (16 septembre 2016, arrêt *Digital Rights Ireland c. Commission,* T-670/16, *JO*, C 410, 7 novembre 2016, p. 26 ; recours déclaré irrecevable par le Tribunal : Ordonnance du Tribunal du 22 novembre 2017) et l'autre par la Quadrature du Net (arrêt *La Quadrature du Net e.a. c. Commission*, T-738/16, *JO*, C 6, 9 janvier 2017, p. 39).

[56] C.J.U.E. (GC), 6 octobre 2015, arrêt *Maximillian Schrems c. Data Protection Commissioner*, C-362/14. Voy. C. DE TERWANGNE et C. GAYREL, « Flux transfrontières de données et exigence de protection adéquate à l'épreuve de la surveillance de masse. Les impacts de l'arrêt Schrems », *Cah. dr. eur.*, 2017, n° 1, pp. 36-81.

[57] En effet, rappelons que la Direction et le RGPD, et donc les décisions d'adéquation de la Commission adoptées sur leur fondement, ne concernent en aucun cas les transferts qui n'entrent pas dans leur champ d'application, en particulier les transferts qui seraient mis en œuvre pour l'exercice d'activités qui ne relèvent pas du champ d'application du droit communautaire, telles que celles prévues aux titres V et VI du Traité sur l'Union européenne, et, en tout état de cause, les traitements ayant pour objet la sécurité publique, la défense, la sûreté de l'État (y compris le bien-être économique de l'État lorsque ces traitements sont liés à des questions de sûreté de l'État) et les activités de l'État relatives à des domaines du droit pénal.

[58] Ainsi que dit au point 3.1.1.b), certaines décisions de la Commission limitent l'autorisation de transferts à certains secteurs. C'est le cas du Canada pour lesquels seuls les transferts vers le secteur privé sont autorisés.

[59] Sauf pour le Privacy Shield pour lequel les entreprises volontaires doivent marquer leur adhésion au Privacy Shield et s'engager auprès du Département du Commerce américain à respecter un ensemble de principes et principes additionnels. Voy. https://www.privacyshield.gov/welcome ; voy. égal. C. BURTON et S. CADIOT, « Règlement général sur la protection des données : les transferts internationaux de données », in B. DOCQUIR (coord.), *Vers un droit européen de la protection des données ?*, Bruxelles, Larcier, 2017, pp. 72-75 ; T. VAN OVERSTRAETEN, « Transborder data flow : today and tomorrow », in N. RAGHENO (coord.) *Data Protection & Privacy. Le GDPR dans la pratique/De GDPR in de praktijk*, Limal, Anthemis, 2017, pp. 152-154.

[60] Commission européenne, « Adequacy of the protection of personal data in non-EU countries », disponible à l'adresse https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_fr.

[61] Art. 45, § 9, du RGPD. Voy. T. VAN OVERSTRAETEN qui parle de « mécanisme de droits acquis », *op. cit.*, p. 153).

§ 3. Les critères à prendre en compte pour évaluer l'adéquation de la protection

16. La Directive ne précisait pas quels critères devaient guider l'évaluation de la protection offerte par un pays tiers. Elle se contentait d'énoncer, à son article 25, que le caractère adéquat du niveau de protection offert devait s'apprécier au regard de toutes les circonstances relatives à un transfert de données ou à une catégorie de transferts.

Le Groupe de l'article 29 avait dès lors mis en place, aux fins d'évaluer l'adéquation du niveau de protection, une méthodologie reprenant les exigences fondamentales que recouvre la notion de protection « adéquate »[62]. Pour le Groupe de l'article 29, l'évaluation du caractère adéquat du niveau de protection devait reposer tant sur une série de critères reprenant des règles de contenu considérées comme essentielles, que sur l'évaluation du dispositif mis en place pour garantir l'efficacité de ces règles. Autrement dit, il devait être tenu compte tant de l'existence des règles en théorie que de leur application et respect dans la pratique.

17. Dans son retentissant arrêt *Schrems*, la Cour de justice s'est penchée pour la première fois sur l'interprétation de l'exigence de protection adéquate des données à caractère personnel lorsque celles-ci sont transférées dans des pays tiers. La Cour, à cette occasion, a considéré que « l'expression 'niveau de protection adéquat' doit être comprise comme exigeant que ce pays tiers assure effectivement, en raison de sa législation interne ou de ses engagements internationaux, *un niveau de protection des libertés et droits fondamentaux substantiellement équivalent* à celui garanti au sein de l'Union en vertu de la directive 95/46, lue à la lumière de la Charte »[63].

À la suite de l'arrêt *Schrems,* les auteurs du RGPD ont complété la notion de niveau adéquat de la protection offerte au-delà des frontières européennes, par les termes empruntés à cet arrêt : le niveau adéquat de protection doit être *essentiellement équivalent*[64] au niveau européen[65]. Cela ne signifie pas que le niveau de protection offert par le régime juridique évalué doive être

[62] Groupe 29, Document de travail « Transferts de données personnelles vers des pays tiers : Application des articles 25 et 26 de la directive relative à la protection des données », adopté le 24 juillet 1998, WP 12.

[63] C.J.U.E. (GC), arrêt *Schrems* précité, pts 73 et 96 (nos italiques).

[64] L'arrêt *Schrems*, précité, au pt 73, évoque un niveau de protection qui doit être « substantiellement équivalent » mais la version anglaise de l'arrêt utilise les termes « *essentially equivalent* ». Ce sont ces derniers termes qui sont repris dans la version anglaise du RGPD, cette fois traduits en français par « essentiellement équivalent ». Il n'y a donc aucune différence à voir entre « essentiellement » et « substantiellement ».

[65] Le considérant n° 104 précise que « [l]e pays tiers devrait offrir des garanties pour assurer un niveau adéquat de protection essentiellement équivalent à celui qui est garanti dans l'Union ».

identique au niveau européen[66]. Ce qui est recherché à travers la notion de protection essentiellement équivalente c'est la continuité du niveau élevé de protection en cas de transfert de données vers un pays tiers[67]. « *[T]he objective is not to mirror point by point the European legislation, but to establish the essential – core requirements of that legislation* »[68]. Les moyens auxquels ce pays tiers a recours pour assurer la protection peuvent être différents de ceux mis en œuvre au sein de l'Union mais ils doivent s'avérer, en pratique, effectifs[69].

Par ailleurs, cet éclairage apporté par la Cour met l'accent sur les objectifs du droit à la protection des données à caractère personnel, en tant que droit instrumental, au service du respect et du renforcement de l'ensemble des libertés et droits fondamentaux[70] À côté du critère « classique » de la protection des données, la Cour consacre le critère, jusqu'ici implicite, de « l'État de droit ». Le RGPD, quant à lui, reprend explicitement ce critère dans les éléments devant être pris en considération par la Commission européenne lorsqu'elle évalue le caractère adéquat ou non de la protection offerte par un pays tiers ou une organisation internationale[71].

18. Les critères énumérés par le règlement pour évaluer le caractère adéquat du niveau de protection comprennent ceux appliqués jusqu'ici et issus du WP 12 du Groupe de l'article 29 évoqué ci-dessus. Ainsi, l'article 45.2 du RGPD invite la Commission à tenir compte des « règles en matière de protection des données, des règles professionnelles et des mesures de sécurité ». Le texte ajoute des éléments plus précis comme les règles relatives aux transferts ultérieurs de données à caractère personnel vers un deuxième pays tiers ou vers une autre organisation internationale ainsi que les droits effectifs et opposables dont bénéficient les personnes concernées.

Outre ces éléments, l'article 45.2 reprend des éléments provenant des règles de procédure. Ainsi, le caractère adéquat de la protection dépend des recours administratifs et judiciaires que peuvent effectivement introduire les personnes concernées dont les données à caractère personnel sont transférées. De même, l'existence d'une ou de plusieurs autorités de contrôle indépendantes

---

66 « Certes, le terme 'adéquat' figurant à l'article 25, paragraphe 6, de la directive 95/46 implique qu'il ne saurait être exigé qu'un pays tiers assure un niveau de protection identique à celui garanti dans l'ordre juridique de l'Union » (C.J.U.E. (GC), 6 octobre 2015, arrêt *Maximillian Schrems c. Data Protection Commissioner*, C-362/14, EU :C :2015 :650, pt 173).

67 C.J.U.E. (GC), arrêt *Schrems* précité, pts 172 et 173.

68 Groupe 29, Adequacy Refential, WP 254 rev. 01, adopted on 6 February 2018, p. 3.

69 *Ibid*.

70 A. Rouvroy et Y. Poullet, « The Right to Informational Self-determination and The Value of Self-Development : Reassessing the Importance of Privacy for Democracy », *Reinventing Data Protection*, Springer, 2009, pp. 45-76.

71 Art. 45, § 2, a), du RGPD : « Lorsqu'elle évalue le caractère adéquat du niveau de protection, la Commission tient compte, en particulier, des éléments suivants : a) l'état de droit, le respect des droits de l'homme et des libertés fondamentales, […] ».

chargées d'assister et de conseiller les personnes concernées dans l'exercice de leurs droits entre dans l'évaluation. Sur ce dernier point, que le RGPD met particulièrement en évidence[72], des compléments sont ajoutés par rapport au WP 12 : l'article 45.2, alinéa b, du RGPD précise qu'il est tenu compte de l'existence d'une ou de plusieurs autorités de contrôle indépendantes dans le pays ou au sein de l'organisation destinataire de données (dont le fonctionnement doit être effectif, il ne peut s'agir d'une autorité de façade), chargées, outre d'aider les personnes concernées à exercer leurs droits, d'assurer le respect des règles en matière de protection des données et de les faire appliquer, ainsi que de coopérer avec les autorités de contrôle des autres États membres. Le texte ne fournit pas d'éclairage sur les critères à prendre en compte pour vérifier l'indépendance des autorités en question. Selon nous, il ne s'agit pas d'appliquer aux autorités extérieures les mêmes critères particulièrement stricts d'indépendance que ceux qui ont été énoncés par la Cour de justice pour les autorités européennes de protection des données[73]. Cette position s'inscrit dans la ligne de la recherche d'une protection hors UE qui soit « essentiellement équivalente » et non identique au régime de l'Union.

Le Groupe de l'article 29 a adopté, le 6 février 2018, un « référentiel pour l'adéquation », document correspondant pour le RGPD à ce que le WP 12 a été pour la Directive, et reprenant tous les principes à respecter pour assurer un niveau adéquat de protection[74]. Ce référentiel distingue les principes de contenu[75] des mécanismes procéduraux et de mise en œuvre[76].

---

[72] Ce point fait l'objet d'un alinéa autonome (b) du paragraphe 2 de l'article 45 du RGPD.

[73] C.J.U.E., 9 mars 2010, arrêt *Commission c. Allemagne*, C518/07, EU:C:2010:125 ; C.J.U.E., 16 octobre 2012, arrêt *Commission c. Autriche*, C-614/10, EU:C:2012:631 ; C.J.U.E., 8 avril 2014, arrêt *Commission c. Hongrie*, C288/12, EU:C:2014:237.

[74] Groupe 29, Adequacy Referential, 6 février 2018, WP 254 rev.01.

[75] Il faut que le système de protection de l'État tiers ou de l'organisation internationale contienne l'exigence de fondements pour le traitement loyal et licite des données, à des fins légitimes ; le principe de finalité ; le principe de qualité des données et de proportionnalité ; le principe de conservation limitée des données ; le principe de sécurité et confidentialité ; le principe de transparence ; les droits d'accès, de rectification, d'effacement et d'objection. Des garanties additionnelles à ces exigences de base doivent être prévues pour les catégories de données dites « sensibles », en matière de marketing direct et pour les décisions entièrement automatisées et le profilage. Enfin, le système juridique doit apporter des restrictions aux transferts ultérieurs des données qui ne peuvent être autorisés que lorsque le destinataire du transfert ultérieur est également soumis à des règles offrant un niveau de protection adéquat.

[76] Le système de protection doit être caractérisé par l'existence et le fonctionnement d'une autorité de contrôle indépendante ; un bon niveau de respect des règles de protection des données ; des obligations pesant sur les responsables de traitement de se conformer aux règles de protection et de démontrer leur conformité ; et des mécanismes pouvant apporter soutien et assistance aux personnes concernées et permettant d'instruire leurs plaintes en fournissant des voies de recours appropriées à la partie lésée en cas de non-respect des règles.

19. Ainsi que dit ci-dessus, d'autres critères ont été ajoutés par le RGPD[77], liés au respect de l'état de droit, au respect des droits de l'homme et des libertés fondamentales, à la législation relative à la sécurité publique, la défense, la sécurité nationale et le droit pénal. À cela a été ajouté en fin de parcours législatif un critère découlant directement de l'arrêt *Schrems* : l'ampleur de l'accès des autorités publiques aux données à caractère personnel.

Sur ce dernier point, le Groupe de l'article 29 a identifié quatre « garanties essentielles » qui offrent les clés pour évaluer le niveau de protection garanti par un pays tiers dans l'exercice de ses activités de surveillance[78]. Il s'agit de l'exigence de légalité de telles activités qui doivent s'opérer dans le cadre de règles claires, précises et accessibles. Il faut ensuite démontrer la nécessité et la proportionnalité des mesures, l'existence d'un mécanisme de supervision indépendant et le droit à un recours effectif. À travers ces quatre garanties essentielles, auxquelles s'ajoute le respect de l'État de droit, c'est la protection substantiellement équivalente ou non des droits fondamentaux qui est mesurée. Ces exigences sont reprises dans le « Adequacy referential » adopté par le Groupe de l'article 29[79].

20. Soulignons que le règlement insiste sur la « mise en œuvre » des législations, ce qui implique de prendre en compte le niveau de protection des droits et libertés conférés *en théorie* et *en pratique* dans l'État tiers concerné.

21. Par ailleurs, une attention particulière doit être portée aux engagements internationaux de l'État. Le considérant n° 105 précise qu'il y a lieu, en particulier, de prendre en considération l'adhésion du pays tiers à la Convention 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel et à son protocole additionnel. L'adhésion à cette convention, même si elle n'est pas déterminante, est « une donnée favorable lors de l'examen du niveau d'adéquation »[80,81].

---

[77] Art. 45.1 du RGPD.

[78] Groupe 29, Working Document 01/2016 on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data (European Essential Guarantees), 16 avril 2016, WP 637.

[79] Groupe 29, Adequacy Referential, 6 février 2018, WP 254 rev.01, chapitre 4.

[80] P. Van Den Bulck, « Transferts de données personnelles vers des pays tiers », *op. cit.*, p. 219.

[81] Voy. la Communication de la Commission au Parlement européen et au Conseil du 10 janvier 2017, Echange et protection de données à caractère personnel à l'ère de la mondialisation, COM(2017)7 final, dans laquelle la Commission annonce qu'elle entend encourager l'adhésion de pays tiers à la Convention 108 du Conseil de l'Europe dans sa version modernisée (pp. 9-10). Aux yeux de la Commission européenne, cette convention, dans

§ 4. Réexamen périodique de la décision d'adéquation

a) Obligation d'examen périodique par la Commission européenne

22. L'acte d'exécution par lequel la Commission reconnait qu'un pays ou une organisation internationale offre une protection adéquate doit prévoir un mécanisme d'examen périodique, au moins tous les quatre ans[82], afin de prendre en compte toutes les évolutions pertinentes, « juridiques, politiques et institutionnelles »[83], qui seraient apparues dans le pays tiers ou au sein de l'organisation internationale depuis la décision d'adéquation.

Cette obligation de réexamen périodique découle de l'expérience tirée de l'affaire *Schrems* dans laquelle il est apparu avec évidence que la situation du pays concerné avait évolué depuis la reconnaissance de l'adéquation de la protection mise en place, en l'occurrence l'instauration du Safe Harbor[84]. Ce sont les révélations d'Edward Snowden sur les pratiques de surveillance généralisée de l'Agence de Sécurité Nationale (NSA – *National Security Agency*) qui sont à l'origine de ce constat qui conduira au spectaculaire coup d'arrêt du Safe Harbor. Après avoir mis au jour les critères d'évaluation du caractère adéquat dont certains sont repris au point précédent, la Cour de justice a en effet relevé que « la Commission n'a pas fait état, dans la décision 2000/520, de ce que les États-Unis d'Amérique 'assurent' effectivement un niveau de protection adéquat en raison de leur législation interne ou de leurs engagements internationaux »[85] alors qu'elle aurait dû justifier que ce pays assure effectivement « un niveau de protection des droits fondamentaux substantiellement équivalent à celui garanti dans l'ordre juridique de l'Union »[86]. La Cour a dès lors invalidé la décision 2000/520 de la Commission instaurant le *Safe Harbor*.

Tirant les enseignements de la situation rencontrée dans cette affaire *Schrems*, le RGPD[87] impose à la Commission européenne de suivre, « de

---

sa version modernisée, reflète « les mêmes principes que ceux consacrés dans les nouvelles règles de l'UE en matière de protection des données, contribuant ainsi à la convergence vers un ensemble de normes élevées en matière de protection des données » (p. 9).

[82] Art. 45, § 3, du RGPD. On notera que la décision mettant en place le Privacy Shield doit être réévaluée tous les ans, « *given the controversial issues surrounding its adoption* » (T. Van Overstraeten, « Transborder data flow : today and tomorrow », in N. Ragheno (coord.) *Data Protection & Privacy. Le GDPR dans la pratique/De GDPR in de praktijk*, Limal, Anthemis, 2017, p. 153).

[83] C. Burton et S. Cadiot, « Règlement général sur la protection des données : les transferts internationaux de données », in B. Docquir (coord.), *Vers un droit européen de la protection des données ?*, Bruxelles, Larcier, 2017, p. 66.

[84] Pt 76 de l'arrêt *Schrems*, précité.

[85] Pt 97 de l'arrêt *Schrems*, précité.

[86] Pt 96 de l'arrêt *Schrems*, précité.

[87] Art. 45, § 4, du RGPD.

façon permanente », sur le plan du droit et des pratiques, les évolutions de l'ordre juridique de l'État ou de l'organisation internationale bénéficiant d'une décision d'adéquation, susceptibles d'entraver le fonctionnement de cette décision, « notamment les évolutions concernant l'accès des autorités publiques aux données à caractère personnel »[88].

b) Consultation et avis préalable

23. L'examen périodique doit être effectué en consultation avec le pays tiers ou l'organisation internationale concernés et en prenant en considération « les observations et les conclusions du Parlement européen et du Conseil, ainsi que d'autres organes et sources pertinents »[89]. Parmi les « autres organes pertinents », on trouvera très vraisemblablement le Contrôleur européen de la protection des données (EDPS)[90].

Avant que la Commission se prononce, le CEPD est également appelé à rendre un avis à propos de la question du maintien ou non d'un niveau de protection adéquat dans le pays tiers ou au sein de l'organisation internationale objet de l'évaluation[91].

c) Abrogation, modification ou suspension de la décision d'adéquation et effet sur les autres instruments de transfert des données

24. L'examen périodique peut déboucher sur l'abrogation, la modification ou la suspension de la décision d'adéquation prise antérieurement[92]. La Commission suit la même procédure pour prendre une telle décision que celle suivie pour adopter la décision d'adéquation. Toutefois, en cas d'urgence dûment justifiée et lorsque des éléments de preuve disponibles montrent que le niveau adéquat de protection est compromis, la Commission peut adopter un acte d'exécution immédiatement applicable[93].

---

[88] Considérant n° 9 de la décision d'exécution (UE) 2016/2295 de la Commission du 16 décembre 2016 modifiant les décisions 2000/518/CE, 2002/2/CE, 2003/490/CE, 2003/821/CE, 2004/411/CE, 2008/393/CE, 2010/146/UE, 2010/625/UE et 2011/61/UE, et les décisions d'exécution 2012/484/UE et 2013/65/UE constatant, conformément à l'article 25, paragraphe 6, de la directive 95/46/CE du Parlement européen et du Conseil, le niveau de protection adéquat des données à caractère personnel assuré par certains pays.

[89] Considérant n° 106 du RGPD.

[90] C. Burton et S. Cadiot, « Règlement général sur la protection des données : les transferts internationaux de données », *op. cit.*, p. 68.

[91] Art. 70, § 1er, s), du RGPD.

[92] Art. 45, § 5, et considérants nos 103 et 107 du RGPD.

[93] Art. 45, § 5, et 93, § 3, et considérant n° 169 du RGPD. Si la Commission est donc dispensée de consulter un comité représentant les États membres, elle devra tout de même

En cas d'abrogation ou de suspension d'une décision d'adéquation, la Commission entame des négociations avec le pays tiers ou l'organisation internationale en cause, en vue de remédier à la situation[94].

25. La décision d'abrogation ou de suspension n'a pas d'effet sur le passé pas plus que sur la validité des autres instruments de transfert des données, tels les règles d'entreprise contraignantes-BCRs ou les clauses contractuelles (décrits *infra*, section 2) qui peuvent toujours être utilisés après le retrait de la reconnaissance de l'adéquation de la protection[95]. Cependant, si le retrait de la décision d'adéquation se base sur des évolutions défavorables sur le plan du respect de l'état de droit et des droits de l'homme ou au niveau de la législation concernant la sécurité nationale et l'accès des autorités publiques aux données au sein de l'État destinataire (comme dans l'affaire *Schrems*), il est douteux que les autres instruments de transfert ne soient pas également impactés et puissent être utilisés. En effet, les BCRs et les clauses contractuelles souffrent des mêmes défauts que ceux du *Safe Harbor* en ce qui concerne les mesures de surveillance[96]. Leurs clauses ne contiennent que des garanties limitées[97] comparables à celles conte-

soumettre la décision prise dans l'urgence à un tel comité dans les quatorze jours qui suivent (art. 8 du règlement 182/2011).

[94] Art. 45, § 6, et considérant n° 107 du RGPD.

[95] Art. 45, § 7, du RGPD. Voy. égal. la communication de la Commission européenne visant à présenter des outils alternatifs pour la réalisation des transferts transatlantiques de données conformément à la directive 95/46/CE en l'absence de décision concernant le caractère adéquat du niveau de protection (Communication de la Commission au Parlement européen et au Conseil concernant le transfert transatlantique de données à caractère personnel conformément à la directive 95/46/CE faisant suite à l'arrêt de la Cour de justice dans l'affaire C-362/14 (*Schrems*), COM/2015/0566 final, 6 novembre 2015).

[96] Ch. Kuner, « Reality and Illusion in EU Data Transfer Regulation Post Schrems », *Legal Studies Research Paper Series*, No. 14/2016, March 2016, pp. 26-28, disponible à l'adresse https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2732346.

[97] Voy. toutefois la lecture que la Commission fait de ces garanties : « tant les CCT que les REC prévoient que si l'importateur de données a des raisons de croire que la législation applicable dans le pays destinataire peut l'empêcher de remplir ses obligations, il est tenu d'en informer immédiatement l'exportateur des données dans l'UE. Dans une telle situation, il appartient à l'exportateur d'envisager la prise des mesures appropriées pour assurer la protection des données à caractère personnel. Celles-ci peuvent aller des mesures techniques, organisationnelles, liées au modèle d'entreprise ou juridiques à la possibilité de suspendre le transfert de données ou de mettre fin au contrat. Tenant compte de toutes les circonstances du transfert, il se peut donc que les exportateurs de données doivent mettre en place des garanties supplémentaires pour compléter celles offertes conformément à la base juridique applicable au transfert de façon à répondre aux exigences de l'article 26, paragraphe 2, de la directive » (Communication de la Commission au Parlement européen et au Conseil concernant le transfert transatlantique de données à caractère personnel conformément à la directive 95/46/CE faisant suite à l'arrêt de la Cour de justice dans l'affaire C-362/14 (*Schrems*), 6 novembre 2015, COM(2015) 566 final, p. 14.

nues dans le *Safe Harbor* et jugées insuffisantes par la Cour de justice[98]. En conséquence, « puisque les risques posés par les pratiques de surveillance excessive en vigueur dans certains pays du monde pourront difficilement être levés dans des BCRs ou clauses contractuelles entre entreprises, de tels instruments alternatifs ne devraient pouvoir être utilisés, selon nous, que pour des transferts vers des *pays sûrs*. Par « pays sûrs », nous proposons d'entendre les pays qui, s'ils ne remplissent pas l'ensemble des conditions nécessaires à une reconnaissance d'adéquation, apportent la démonstration du respect des « garanties essentielles » énoncées par le Groupe de l'article 29 dans le domaine de la surveillance »[99]. Ainsi que dit plus haut, quatre garanties essentielles ont été identifiées, à la suite de l'arrêt *Schrems*, pour évaluer le niveau de protection garanti par un pays tiers dans le cadre de ses activités de surveillance[100]. Les flux de données vers les pays tiers respectant ces garanties essentielles ainsi que l'état de droit peuvent donc être réalisés en recourant aux instruments alternatifs que sont les clauses contractuelles et les BCR mais également aux autres instruments permettant de réaliser des transferts de données à caractère personnel aux termes de l'article 46 du RGPD (voy. *infra*, section 2).

Cela étant, les exceptions prévues à l'article 49 du RGPD peuvent toujours être invoquées pour valider les transferts qui ne sont pas massifs ni structurels, que ce soit vers un pays offrant une protection reconnue comme adéquate ou non et pouvant être qualifié de pays sûr ou non.

---

[98] Concernant l'impact sur les clauses contractuelles types des accès excessifs des autorités publiques aux données transférées, voy. la décision de la Haute Cour irlandaise du 3 octobre 2017, dans une affaire initiée par une (nouvelle) plainte de Max Schrems, de saisir la C.J.U.E. d'une question préjudicielle sur l'adéquation du niveau de protection offert par les clauses contractuelles types et dès lors sur la validité de ces clauses ; voy. I. CUNNINGHAM, « La Haute Cour saisit la Cour de justice de l'Union européenne d'une question préjudicielle dans l'affaire Facebook c. Irlande », *IRIS*, 2017-10 :1/22, http://merlin.obs.coe.int/iris/2017/10/article 22.fr.html ; S. PEYROU, « Transfert de données à caractère personnel UE-États Unis : nouvel épisode du feuilleton 'Privacy Shield' (Réflexions à propos du rapport du Groupe de l'article 29 relatif au premier examen annuel conjoint du Privacy Shield, WP 255) », 1er janvier 2018, http://www.gdr-elsj.eu/2018/01/01/informations-generales/transfert-de-donnees-a-caractere-personnel-ue-etats-unis-nouvel-episode-du-feuilleton-privacy-shield-reflexions-a-propos-du-rapport-du-groupe-de-larticle-29-re/.

[99] C. DE TERWANGNE et C. GAYREL, « Flux transfrontières de données et exigence de protection adéquate à l'épreuve de la surveillance de masse. Les impacts de l'arrêt Schrems », *op. cit.*, p. 77.

[100] Voy. *supra*, § 19.

§ 5. Pouvoir d'intervention des autorités nationales ?

26. La Cour de justice a précisé, à l'occasion de son arrêt *Schrems,* que les autorités nationales de contrôle demeurent compétentes pour contrôler le transfert de données à caractère personnel vers un pays tiers ayant fait l'objet d'une décision d'adéquation de la Commission[101]. Cette dernière ne peut réduire les pouvoirs reconnus à ces autorités nationales de contrôle, comme elle l'avait fait dans sa décision d'adéquation mettant en place le Safe Harbor, ainsi que dans plusieurs autres décisions d'adéquation[102].

Toutefois, les décisions d'adéquation de la Commission ont un caractère contraignant pour ces autorités de contrôle, en ce qu'elles autorisent les transferts de données à caractère personnel depuis l'Union européenne vers le pays tiers ou l'organisation internationale visés par ces décisions[103]. Les autorités nationales de contrôle ne peuvent en conséquence invalider ces décisions ou estimer qu'un pays tiers visé par une décision d'adéquation n'assure en réalité pas un niveau de protection adéquat. Comme l'a précisé l'arrêt *Schrems*, cela n'empêche pas, au demeurant, une autorité nationale de contrôle d'examiner la demande d'une personne relative au niveau de protection de ses données à caractère personnel assuré dans un pays tiers visé par une décision d'adéquation de la Commission et, le cas échéant, d'engager un recours devant les juridictions nationales afin que ces dernières, si elles partagent les doutes de cette autorité quant à la validité de la décision de la Commission, procèdent à un renvoi préjudiciel aux fins de l'examen de la validité de cette décision par la Cour de justice[104].

---

[101] C.J.U.E. (GC), arrêt *Schrems*, précité, pts 47, 53, 57 et 63. P. Van Den Bulck, « Transferts de données personnelles vers des pays tiers », *op. cit.*, pp. 222-223.

[102] En conséquence, la Commission a adopté la décision d'exécution (UE) 2016/2295 du 16 décembre 2016 modifiant les décisions 2000/518/CE, 2002/2/CE, 2003/490/CE, 2003/821/CE, 2004/411/CE, 2008/393/CE, 2010/146/UE, 2010/625/UE et 2011/61/UE, et les décisions d'exécution 2012/484/UE et 2013/65/UE constatant, conformément à l'article 25, paragraphe 6, de la directive 95/46/CE du Parlement européen et du Conseil, le niveau de protection adéquat des données à caractère personnel assuré par certains pays.

[103] C.J.U.E. (GC), arrêt *Schrems*, précité, pts 51, 52 et 62.

[104] C.J.U.E. (GC), arrêt *Schrems*, précité, pts 52, 62 et 65 et considérants n^{os} 3 à 6 de la décision d'exécution (UE) 2016/2295 de la Commission du 16 décembre 2016 modifiant les décisions 2000/518/CE, 2002/2/CE, 2003/490/CE, 2003/821/CE, 2004/411/CE, 2008/393/CE, 2010/146/UE, 2010/625/UE et 2011/61/UE, et les décisions d'exécution 2012/484/UE et 2013/65/UE constatant, conformément à l'article 25, paragraphe 6, de la directive 95/46/CE du Parlement européen et du Conseil, le niveau de protection adéquat des données à caractère personnel assuré par certains pays.

SECTION 2. – Le transfert encadré par des garanties appropriées (art. 46 et 47 du RGPD)

27. Dans les cas où le responsable de traitement ou le sous-traitant établi dans l'Union européenne envisage de transférer des données à caractère personnel vers un État tiers ou une organisation internationale n'offrant pas une protection reconnue comme adéquate par la Commission européenne (soit tous les autres pays que ceux repris dans la liste blanche de la Commission), il doit lui-même assurer que les transferts envisagés sont assortis de garanties appropriées.

Ces garanties appropriées peuvent résulter de divers mécanismes « qui sont suffisamment souples pour s'adapter à une variété de situations de transfert différentes »[105]. Il est vrai que la palette des mécanismes à la disposition des acteurs est plus large dans le RGPD que dans le régime précédent. Il s'agit des clauses contractuelles (clauses contractuelles types proposées par la Commission européenne[106] ou par une autorité de contrôle[107] ou clauses contractuelles *ad hoc*[108]) ou des règles d'entreprises contraignantes[109] (en anglais *Binding Corporate Rules*), instruments familiers car déjà disponibles sous le régime de la Directive et que le RGPD reconnait officiellement en les incorporant. Mais ces garanties peuvent également prendre des formes nouvelles : elles peuvent être insérées dans des codes de conduite[110] ou des mécanismes de certification[111] ou, s'agissant de transferts impliquant des autorités ou organismes publics, dans des instruments spécifiques[112].

On notera que la faculté d'autoriser des transferts internationaux moyennant des garanties appropriées n'est pas une compétence exclusive de la Commission européenne mais, sur certains points (voy. ci-dessous), est une compétence partagée avec les États Membres.

28. Le RGPD précise qu'on ne peut avoir recours à cette voie des garanties appropriées pour encadrer les flux transfrontières de données et compenser l'insuffisance de la protection offerte dans le pays tiers, qu'à la

[105] Communication de la Commission au Parlement et au Conseil du 10 janvier 2017, Echange et protection de données à caractère personnel à l'ère de la mondialisation, COM(2017)7 final, p. 8.
[106] Art. 46, § 2, c), du RGPD.
[107] Art. 46, § 2, d), du RGPD.
[108] Art. 46, § 3, a), du RGPD.
[109] Art. 46, § 2, b), et art. 47 du RGPD.
[110] Art. 46, § 2, e), du RGPD.
[111] Art. 46, § 2, f), du RGPD.
[112] Art. 46, § 2, a), et § 3, c), du RGPD.

condition « que les personnes concernées disposent de droits opposables et de voies de droit effectives »[113]. Le considérant n° 108 précise que les garanties appropriées « devraient assurer […] l'existence de droits opposables de la personne concernée et de voies de droit effectives, ce qui comprend le droit d'engager un recours administratif ou juridictionnel effectif et d'introduire une action en réparation, dans l'Union ou dans un pays tiers ».

29. Enfin, puisque l'on envisage ici les transferts de données vers des destinations n'offrant pas de protection adéquate, il convient de faire une remarque : le RGPD a prévu que, dans ces cas, les États membres ou l'Union européenne peuvent restreindre, pour des motifs importants d'intérêt public, les transferts de *données sensibles* vers un pays ou une organisation internationale n'ayant pas bénéficié d'une décision d'adéquation[114].

§ 1. Clauses contractuelles types

30. Conformément à ses prérogatives découlant déjà de la Directive, la Commission européenne a adopté plusieurs modèles de clauses contractuelles types, considérées comme apportant des « garanties appropriées ». L'on distingue les clauses contractuelles types qui intéressent les transferts internationaux entre un responsable de traitement établi dans l'Union et un autre responsable de traitement établi dans un État tiers (CCT « responsable de traitement à responsable de traitement ») (point a, ci-dessous) des clauses contractuelles types applicables aux transferts d'un responsable de traitement dans l'Union vers un sous-traitant dans un État tiers (CCT « responsable de traitement à sous-traitant ») (point b, ci-dessous). Aux fins de déterminer les clauses appropriées, il est donc essentiel d'identifier la qualité du destinataire des données[115]. On relèvera que « [d]ans tous les cas, l'utilisation de clauses contractuelles suppose que la société exportatrice de données ait un établissement dans un pays de l'UE »[116].

Les différents types de clauses contractuelles considérées sous l'empire de la Directive comme offrant des garanties appropriées pour autoriser les transferts de données à caractère personnel hors de l'UE sont actuellement l'objet de révision afin d'être mises en conformité avec le RGPD. Les ajustements qui découleront de cette révision ne devraient cependant pas aboutir

[113] Art. 46, § 1er, du RGPD.

[114] Art. 49, § 5, du RGPD.

[115] Pour ce, voy. les sections consacrées aux notions de « responsable de traitement » et de « sous-traitant » dans la contribution de C. DE TERWANGNE dans le présent ouvrage « Définitions clés et champ d'application du RGPD ».

[116] C. BURTON et S. CADIOT, « Règlement général sur la protection des données : les transferts internationaux de données », *op. cit.*, p. 78.

à des modifications substantielles de ces instruments qui ont connu un grand succès jusqu'à présent. L'article 46, § 5, du RGPD prévoit que ces clauses demeurent en vigueur jusqu'à leur modification ou leur éventuel remplacement ou abrogation, « *grandfathering system* »[117] bienvenu pour les nombreux intervenants qui se sont appuyés sur ces clauses pour légaliser leurs transferts de données, spécialement après l'arrêt *Schrems*[118].

31. Le RGPD prévoit que des clauses types de protection des données peuvent également être adoptées par une autorité de contrôle nationale et approuvées par la Commission européenne[119]. Cette approbation doit être faite en conformité avec la procédure d'examen prévue à l'article 5 du règlement 182/2011[120]. Ainsi, avant d'approuver un jeu de clauses types, la Commission doit recevoir l'approbation d'un comité composé des représentants des États membres de l'UE. Le CEPD est précédemment appelé à donner son avis sur le projet de décision de l'autorité de contrôle[121].

32. Ces clauses types présentent le grand intérêt de dispenser de toute procédure d'autorisation auprès d'une autorité de contrôle[122]. Elles se différencient en cela des clauses *ad hoc* qui sont aussi admises pour encadrer des flux transfrontières de données mais doivent être approuvées par une autorité de contrôle (voy. *infra*, § 2).

a) CCT de responsable de traitement à responsable de traitement

33. La Commission européenne propose deux ensembles de clauses, adoptées respectivement en 2001[123] et 2004[124], pour les transferts d'un responsable de traitement vers un autre responsable de traitement établi dans un pays tiers. Ces derniers sont libres d'utiliser l'un ou l'autre ensemble de clauses.

---

[117] T. Van Overstraeten, « Transborder data flow : today and tomorrow », *op. cit.*, p. 154.

[118] *Ibid.*, pp. 154-155.

[119] Art. 46, § 2, d), du RGPD.

[120] Règlement 182/2011 établissant les règles et principes généraux relatifs aux modalités de contrôle par les États membres de l'exercice des compétences d'exécution par la Commission, *J.O.U.E.*, L 55/13.

[121] Art. 64, § 1er, d), du RGPD.

[122] Art. 46, § 2, du RGPD.

[123] Décision 2001/497/CE de la Commission du 15 juin 2001 approuvant les clauses contractuelles types aux fins de l'article 26, paragraphe 2, de la directive 95/46/CE pour le transfert de données à caractère personnel vers des pays tiers qui n'assurent pas un niveau adéquat de protection, *J.O.C.E.*, L 181 du 4 juillet 2001.

[124] Décision 2004/915/CE de la Commission du 27 décembre 2004 introduisant un ensemble alternatif de clauses contractuelles types pour le transfert de données à caractère personnel vers des pays tiers qui n'assurent pas un niveau adéquat de protection, *J.O.U.E.*, L 385 du 29 décembre 2004.

Ces deux jeux de clauses précisent les obligations respectives des deux parties, à savoir l'exportateur et l'importateur de données à caractère personnel. Ces clauses se caractérisent en particulier par le fait qu'elles contiennent la clause dite du « tiers bénéficiaire » qui consiste à permettre aux personnes dont les données sont transférées de se prévaloir des termes du contrat, quand bien même elles n'y sont pas formellement parties, dans les cas où elles subiraient un dommage du fait du non-respect par l'une des parties de ses obligations[125].

Aux obligations déjà prévues dans les clauses de 2001, celles de 2004 ajoutent des obligations de diligence plus détaillées, notamment concernant l'importateur. L'importateur est ainsi expressément tenu de s'engager à mettre en place des mesures techniques et organisationnelles pour protéger les données (principe de sécurité), de mettre en place des procédures assurant que les tiers y compris les sous-traitant accédant aux données respectent et préservent la confidentialité de celles-ci, de désigner un point de contact pour répondre aux demandes de l'exportateur ; d'apporter la preuve qu'il dispose des ressources financières suffisantes pour assumer ses responsabilités[126]. Le transfert ultérieur par l'importateur des données à un autre responsable de traitement situé dans un pays en dehors de l'EEE est explicitement soumis aux conditions suivantes : soit le destinataire est établi dans un pays offrant une protection adéquate suivant une décision de la Commission, soit il devient lui-même signataire des clauses contractuelles types, soit les personnes concernées ont été informées du transfert et ont eu la possibilité d'exercer leur droit d'opposition. Enfin, le consentement explicite des personnes concernées est requis en cas de transferts ultérieurs de données sensibles.

C'est essentiellement le régime de responsabilité qui distingue les clauses de 2004 de celles de 2001. Tandis que les premières établissent un régime de responsabilité solidaire (en cas de dommage, la personne concernée étant libre de poursuivre l'importateur ou l'exportateur des données, ou les deux en même temps[127]), les secondes établissent un régime de responsabilité reposant sur des obligations de diligence, selon lequel l'exportateur et l'importateur des données sont responsables, vis-à-vis des personnes concernées, de leurs manquements respectifs à leurs obligations contractuelles. L'exercice des droits du tiers bénéficiaire par les personnes concernées prévoit une implication plus importante de l'exportateur de données. En cas d'allégation de manquement dans le chef de l'importateur de données, la personne concernée doit s'adresser en premier lieu à l'exportateur, qui est

[125] Clause 3 « du Tiers bénéficiaire ».
[126] Clause II « Obligations de l'importateur de données ».
[127] Clause 6 « Responsabilité ».

tenu d'entreprendre des démarches auprès de l'importateur pour faire valoir ses obligations. Si le manquement se poursuit ou bien si l'exportateur n'entreprend pas les démarches nécessaires pour y faire remédier dans un délai d'un mois, le tiers bénéficiaire peut poursuivre directement l'importateur devant la juridiction communautaire d'établissement de l'exportateur[128].

b) CCT de responsable de traitement à sous-traitant

34. La Commission européenne a approuvé des clauses contractuelles types spécifiques aux transferts d'un responsable de traitement établi dans l'Union à un sous-traitant situé dans un État tiers n'offrant pas de protection adéquate. Un premier ensemble de clauses a été adopté en 2001, puis mis à jour en 2010 à la lumière de l'expérience acquise, des développements technologiques et aux fins d'adapter les obligations des parties à des chaînes de sous-traitance toujours plus complexes[129].

Conformément au principe de la Directive repris dans le RGPD, les clauses rappellent l'obligation pour l'importateur sous-traitant de traiter les données pour le compte exclusif de l'exportateur et selon ses instructions[130], et le devoir pour l'exportateur de s'en assurer[131]. Les traitements, y compris le transfert, continuent d'être effectués conformément au droit applicable à la protection des données du lieu d'établissement du responsable de traitement[132]. En cas de résiliation du contrat, l'importateur est soumis à l'obligation de restituer l'ensemble des données ou de les détruire[133].

Les clauses prévoient par ailleurs l'obligation pour l'importateur de mettre en œuvre les mesures techniques et organisationnelles propres à assurer la sécurité des données[134]. En outre, l'importateur est tenu de notifier à l'exportateur toute atteinte à la sécurité des données, ainsi que les demandes contraignantes de divulgation des données émanant d'autorité de maintien de l'ordre[135].

---

[128] Clause III « Responsabilité et droits des tiers ».

[129] Décision de la Commission 2010/87/UE du 5 février 2010 relative aux clauses contractuelles types pour le transfert de données vers des sous-traitants établis dans des pays tiers en vertu de la directive 95/46/CE du Parlement européen et du Conseil, *J.O.U.E.*, L 39 du 12 février 2010.

[130] Clause 5, a), « Obligations de l'importateur de données ».

[131] Clause 4, b), « Obligations de l'exportateur de données ».

[132] Clause 4, a), « Obligations de l'exportateur de données ».

[133] Clause 12 « Obligation après la résiliation des services de traitement des données à caractère personnel ».

[134] Clause 5, c), « Obligations de l'importateur de données » et clause 1 f) définition de « mesures techniques et d'organisation liées à la sécurité ».

[135] Clause 5, d), « Obligations de l'importateur de données ».

Toute sous-traitance ultérieure par l'importateur est soumise à l'accord écrit préalable de l'exportateur et à la signature d'un accord écrit imposant au sous-traitant ultérieur les mêmes obligations que celles qui incombent à l'importateur en application des clauses[136].

L'importateur est enfin tenu d'accepter de soumettre ses moyens de traitement à un éventuel audit, sur demande de l'exportateur[137]. L'autorité de contrôle du lieu d'établissement de l'exportateur de données dispose en outre du droit d'effectuer directement des vérifications chez l'importateur de données ou chez le sous-traitant ultérieur[138].

Au niveau du régime de responsabilité, ces CCT établissent en premier lieu la responsabilité de l'exportateur de données en cas de dommages pour les personnes concernées. Celles-ci, en tant que tiers bénéficiaires, ont le droit d'obtenir réparation auprès du responsable de traitement du préjudice subi, et ce même en cas de manquement de l'importateur ou du sous-traitant ultérieur[139]. En cas d'impossibilité de poursuivre le responsable de traitement (lorsque celui-ci a matériellement disparu, cessé d'exister en droit ou est devenu insolvable), la personne concernée a le droit d'obtenir réparation auprès de l'importateur. Dans ce cas, il est prévu que la personne concernée puisse porter le litige devant la juridiction compétente de l'État membre où l'exportateur est établi[140].

§ 2. Clauses contractuelles *ad hoc* soumises à autorisation

35. Des clauses contractuelles *ad hoc* peuvent être élaborées par le responsable de traitement ou le sous-traitant qui ne souhaite pas accompagner le transfert de données de clauses « conformes » aux clauses types. Par « conformes », on entend des « clauses identiques aux clauses types » ou des « clauses marginalement modifiées » par rapport aux clauses types (sur le plan de la ponctuation ou de la traduction)[141]. Il s'agit donc ici de clauses « taillées sur mesure » pour être adaptées à des cas concrets qui ne peuvent se satisfaire des clauses types existantes.

[136] Clause 5, h), « Obligations de l'importateur de données » et Clause 11 « Sous-traitance ultérieure ».

[137] Clause 5, f), Obligations de l'importateur de données ».

[138] Clause 8, § 1, « Coopération avec les autorités de contrôle ».

[139] Clause 6 « responsabilité ».

[140] Clause 7 « Médiation et juridiction ».

[141] Pour reprendre l'explication donnée par l'art. 8 du Protocole d'accord signé le 25 juin 2013 entre la Commission belge de la protection de la vie privée et le Ministère de la Justice relatif aux clauses contractuelles.

Ces clauses *ad hoc* doivent être autorisées par l'autorité de contrôle compétente[142] qui doit auparavant recueillir l'avis du Comité européen de la protection des données[143], ce qui les rend de toute évidence moins attrayantes que les clauses types, déjà prêtes à l'emploi[144].

Aux fins d'évaluer le niveau de protection des données offert par les clauses *ad hoc* qui lui sont soumises, l'autorité de contrôle se fondera sans doute à l'avenir, comme elle le faisait jusqu'à présent[145], sur les principes énoncés par le Groupe de l'article 29 dans son document relatif aux transferts de données vers des pays tiers, le « référentiel pour l'adéquation »[146]. Ainsi, les autorités de contrôle veilleront à ce que les clauses proposées contiennent l'obligation pour les parties de respecter l'ensemble des principes fondamentaux de la protection des données : principe de finalité et interdiction de traitement ultérieur incompatible ; qualité et proportionnalité des données ; transparence du traitement ; sécurité des données ; droits d'accès, de rectification et d'opposition ; restrictions aux transferts ultérieurs ; ainsi que des garanties supplémentaires concernant le traitement des données sensibles, le marketing direct et les décisions automatisées. L'autorité de contrôle devrait aussi évaluer l'efficacité de ces règles de fond au regard de trois objectifs[147] : assurer un niveau satisfaisant des règles ; fournir une assistance et une aide aux personnes concernées dans l'exercice de leurs droits ; offrir des voies de recours appropriées à la personne concernée en cas d'inobservation des règles.

---

[142] Art. 46, § 3, du RGPD.

[143] Art. 64, § 1er, e), du RGPD. Afin de contribuer à la cohérence dans l'application du RGPD, les autorités de contrôle appelées à se prononcer sur des clauses *ad hoc* doivent coopérer entre elles et, le cas échéant, avec la Commission européenne (art. 46, § 4, du RGPD) à travers le « mécanisme de contrôle de la cohérence » (mécanisme établi à l'article 63 du RGPD).

[144] Cédric Burton et Sarah Cadiot relèvent que par le passé, ces clauses déjà soumises à un régime d'autorisation, ont été moins utilisées que les clauses types (C. Burton et S. Cadiot, « Règlement général sur la protection des données : les transferts internationaux de données », *op. cit.*, p. 80).

[145] Voy. pour la pratique belge avant la mise en application du RGPD, l'article 5 du Protocole d'accord relatif aux clauses contractuelles du 25 juin 2013, précité, renvoyant au WP12 du Groupe 29.

[146] Groupe 29, Adequacy Referential, 6 février 2018, WP 254 rev.01 (voy. *supra).*

[147] Ce sont les trois objectifs identifiés par le Groupe 29 et servant à l'évaluation du caractère adéquat du niveau de protection des données offert dans un pays tiers.

§ 3. Règles d'entreprise contraignantes

a) Définition et avantages

36. Les règles d'entreprise contraignantes (plus communément désignées sous leur acronyme anglais « BCR » – *Binding Corporate Rules*) désignent un code de conduite interne qui définit la politique d'un groupe en matière de transferts de données personnelles en dehors de l'Union européenne. Elles sont plus précisément définies à l'article 4.20 du RGPD comme étant « les règles internes relatives à la protection des données à caractère personnel qu'applique un responsable du traitement ou un sous-traitant établi sur le territoire d'un État membre de l'Union aux transferts ou à un ensemble de transferts de données à caractère personnel à un responsable du traitement ou à un sous-traitant dans un ou plusieurs pays tiers au sein d'un groupe d'entreprises ou d'un groupe d'entreprises engagées dans une activité économique conjointe ».

37. Les règles d'entreprise contraignantes constituent une alternative intéressante aux clauses contractuelles type puisqu'elles permettent d'assurer un niveau de protection approprié aux données à caractère personnel transférées qui peuvent dès lors circuler librement au sein du groupe d'entreprises ou d'un groupe d'entreprises engagées dans une activité économique conjointe[148]. Elles représentent un outil précieux au service d'« une politique de protection des données robuste qui s'incorpore dans l'ADN du groupe »[149]. C'est « la solution la plus pérenne parmi tous les mécanismes de transferts », elles « instaurent une vraie culture de protection des données au sein d'un groupe d'entreprises »[150]. Même si elles sont lourdes à élaborer et faire approuver, elles présentent d'évidents avantages : « uniformiser les pratiques au sein du groupe ; prévenir les risques inhérents aux transferts vers les pays tiers ; éviter de conclure autant de contrats qu'il existe de transferts ; avoir un seul document pour l'ensemble des sociétés concernées ; faciliter le processus d'autorisation des traitements impliquant des transferts internationaux ; placer la protection des données au rang des préoccupations éthiques du groupe et pouvoir communiquer sur cette politique auprès des clients, partenaires et salariés »[151].

---

[148] C. Burton et S. Cadiot, « Règlement général sur la protection des données : les transferts internationaux de données », *op. cit.*, p. 76.

[149] P. Van Den Bulck, « Transferts de données personnelles vers des pays tiers », *op. cit.*, p. 226.

[150] C. Burton et S. Cadiot, « Règlement général sur la protection des données : les transferts internationaux de données », *op. cit.*, p. 77.

[151] A. Bensoussan (dir.), *La protection des données personnelles de A à Z*, coll. Abécédaires, Bruxelles, Bruylant, 2017, p. 202, n° 1007.

Le Groupe de l'article 29 a progressivement adopté toute une série d'avis utiles relatifs aux règles d'entreprise contraignantes, portant tant sur le contenu que sur la forme ou sur la procédure d'autorisation de ces BCR. Ces avis ont été revus pour être mis en conformité avec le RGPD[152] et ces dernières versions ont été approuvées par l'EDPB[153].

b) Exportateurs de données admis à avoir recours aux règles d'entreprise contraignantes

38. Le « groupe d'entreprises », acteur visé par les règles d'entreprise contraignantes, est défini comme composé d'« une entreprise qui exerce le contrôle et [des] entreprises qu'elle contrôle »[154], l'entreprise étant entendue comme « une personne physique ou morale exerçant une activité économique, quelle que soit sa forme juridique, y compris les sociétés de personnes ou les associations qui exercent régulièrement une activité économique »[155]. Le considérant n° 37 du RGPD apporte cette précision qu'un groupe d'entreprises devrait consister en « une entreprise qui exerce le contrôle et ses entreprises contrôlées, la première devant être celle qui peut exercer une influence dominante sur les autres entreprises du fait, par exemple, de la détention du capital, d'une participation financière ou des règles qui la régissent, ou du pouvoir de faire appliquer les règles relatives à la protection des données à caractère personnel ». La notion de « groupe d'entreprises » couvre donc l'entité formée d'une entreprise qui contrôle le traitement de données à caractère personnel dans des entreprises qui lui sont affiliées. Le considérant n° 48 du RGPD évoque, quant à lui, des « établissements affiliés à un organisme central ».

39. Les entreprises concernées par la souscription volontaire à des règles d'entreprise contraignantes sont essentiellement les multinationales exportant des données depuis leurs entités situées dans l'Union européenne vers

[152] Groupe 29, Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules, WP 256 rev.01 ; Working Document setting up a table with the elements and principles to be found in Processor Binding Corporate Rules, as last revised and adopted on 6 February 2018, WP 257 rev.01 ; Recommendation on the Standard Application for Approval of Controller Binding Corporate Rules for the Transfer of Personal Data, 11 avril 2018, WP 264 ; Working document setting forth a co-operation procedure for the approval of « Binding Corporate Rules » for controllers and processors under the GDPR, 11 avril 2018, WP 263 rev.01 et Recommendation on the Standard Application form for Approval of Binding Corporate Rules for the Transfer of Personal Data, 11 avril 2018, WP 265.

[153] Voy. EDPB, Endorsement 1/2018 of GDPR WP29 guidelines by the EDPB, 25 May 2018, https://edpb.europa.eu/news/news/2018/endorsement-gdpr-wp29-guidelines-edpb_en.

[154] Art. 4.19 du RGPD.

[155] Art. 4.18 du RGPD.

des entités situées dans des pays tiers n'offrant pas un niveau de protection adéquat. En effet, les sociétés multinationales sont en général composées d'entités étroitement liées et hiérarchisées permettant l'application globale d'un code de conduite contraignant tel que celui des règles d'entreprise contraignantes. Toutefois on a vu que « de plus en plus d'entreprises de taille intermédiaire dont les activités nécessitent d'importants flux internationaux de données (par exemple, dans le domaine de l'informatique en nuage ou *cloud computing*) optent également pour les BCRs »[156].

À titre d'illustration de groupes d'entreprises qui ont opté pour le recours aux BCR pour encadrer leurs flux de données intra-groupe, on citera American Express, BNP Paribas, DocuSign, MasterCard, Lego, Linklaters, Safran, Total, Siemens, etc[157]..

40. Le RGPD a intégré une autre catégorie d'utilisateurs potentiels des BCR : les ensembles d'entreprises qui participent à une activité économique conjointe mais ne font pas nécessairement partie du même groupe[158]. La Commission a donné l'exemple du secteur du voyage pour illustrer ces ensembles d'entreprises qui ne sont pas intégrées comme des multinationales mais présentent les mêmes besoins sectoriels[159].

41. On signalera encore que les transferts d'une entité du groupe (que ce groupe soit une multinationale ou un groupe d'intérêts communs) vers une entreprise extérieure au groupe ne sont pas couverts par les Règles d'entreprise contraignantes. De tels transferts sont des transferts ultérieurs de données qui doivent être assortis de garanties suffisantes, telles que des CCT ou des clauses *ad hoc*.

c) Éléments essentiels des règles d'entreprise contraignantes

42. Les BCR doivent être juridiquement contraignantes et respectées par toutes les entités d'un groupe, quel que soit leur pays d'implantation, ainsi que par tous leurs employés[160]. Toutefois, le Groupe de l'article 29 a admis qu'il peut y avoir une distinction légitime entre les données provenant de

---

[156] C. Burton et S. Cadiot, « Règlement général sur la protection des données : les transferts internationaux de données », *op. cit.*, pp. 76-77.

[157] Commission européenne, « List of companies for which the EU BCR cooperation procedure is closed", 24 mai 2018, accessible à l'adresse http://ec.europa.eu/newsroom/article 29/item-detail.cfm?item_id=613841.

[158] Art. 47, § 1er, a), du RGPD.

[159] Communication de la Commission au Parlement européen et au Conseil du 10 janvier 2017, Echange et protection de données à caractère personnel à l'ère de la mondialisation, COM(2017)7 final, p. 8.

[160] Art. 47, § 1er, a), du RGPD.

l'UE et d'autres catégories de données[161]. En effet, le caractère exécutoire des règles ne peut viser que les données transférées au départ de l'UE et pour lesquelles le régime européen des flux transfrontières est d'application.

43. Les BCR doivent conférer expressément aux personnes concernées des droits opposables[162]. C'est la clause du tiers bénéficiaire, clause clé dans l'édifice de protection basé sur les BCR.

44. L'article 47 du RGPD dédié aux règles d'entreprises contraignantes liste quatorze éléments qui doivent être présents dans les BCR et qui découlent des documents adoptés par le Groupe de l'article 29 avant l'avènement du RGPD, avec « *some subtle differences* »[163].

Les garanties appropriées apportées par les règles d'entreprise contraignantes s'apprécient en premier lieu au regard des principes de protection des données. Ainsi, les Règles proposées doivent contenir l'obligation pour les parties de respecter l'ensemble des principes fondamentaux de la protection des données : principe de finalité et interdiction de traitement ultérieur incompatible ; qualité et proportionnalité des données ; limitation des durées de conservation des données ; traitement des données sensibles ; sécurité des données ; restrictions aux transferts ultérieurs[164]. Le RGPD a jouté le respect du principe de *privacy by design* et *by default* et exige aussi l'indication de la base juridique du traitement.

Les BCR doivent encore garantir des droits aux personnes concernées[165], notamment concernant le marketing direct et les décisions automatisées, ainsi que le droit de réclamation, de recours et le droit à indemnisation en cas de violation du RGPD. Les Règles d'entreprise contraignantes doivent en effet prévoir que les personnes concernées ont un droit de réclamation, à leur choix, soit auprès d'une autorité de protection des données dans l'État membre de leur résidence habituelle, de leur lieu de travail ou du lieu où la violation aurait été commise, soit auprès d'un tribunal compétent situé sur le territoire de l'Union européenne. Ce tribunal compétent sera soit celui de l'État membre où la personne concernée a sa résidence habituelle, soit celui de l'État membre où se situe l'entité exportatrice des données[166].

---

[161] Groupe 29, Document de travail sur les questions fréquemment posées (FAQ) concernant les règles d'entreprise contraignantes, WP 74, adopté le 24 juin 2008 révisé et adopté le 8 avril 2009, p. 7.

[162] Art. 47, § 1er, b), du RGPD.

[163] T. Van Overstraeten, « Transborder data flow : today and tomorrow », *op. cit.*, p. 155.

[164] Art. 47, § 2, d), du RGPD.

[165] Art. 47, § 2, e), du RGPD.

[166] Groupe 29, Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules, WP 256 rev.01 ; Working Document setting up a table with the elements and principles to be found in Processor Binding Corporate Rules, 6 février 2018, WP 257 rev.01.

Un nouvel élément important consiste dans l'obligation de prévoir dans les BCR un engagement à communiquer à l'autorité de contrôle compétente toutes les obligations juridiques auxquelles une entité du groupe d'entreprises, ou du groupe d'entreprises engagées dans une activité économique conjointe, est soumise dans un pays tiers, qui sont susceptibles d'avoir un effet négatif important sur les garanties fournies par les BCR[167], à moins qu'une telle communication soit interdite comme dans le cas d'une interdiction pénale afin de préserver la confidentialité d'une enquête pénale[168]. Le Groupe de l'article 29 a précisé que cela inclut toute demande contraignante de divulgation provenant d'autorités de police, de services répressifs ou de services de sûreté de l'État[169].

d) Procédure d'autorisation

45. Le groupe d'entreprises, qu'il s'agisse d'une multinationale ou d'un groupe d'entreprises engagées dans une activité économique conjointe, doit soumettre son projet de règles d'entreprise contraignantes à l'autorité de contrôle compétente pour faire approuver les règles en question.

Si le groupe comprend plusieurs entités établies sur le territoire européen, la procédure d'approbation peut impliquer plusieurs autorités de contrôle. Toutefois le RGPD n'a pas prévu de règles pour organiser la coopération de ces autorités en pareil cas, pas plus qu'il n'a donné d'indication pour désigner une autorité « chef de file » spécifique pour les BCR, une « BCR lead »[170]. Le Groupe de l'article 29 a dès lors adopté, le 11 avril 2018, un document de travail destiné à clarifier la procédure de coopération entre autorités de contrôle pour l'approbation des projets de BCR et la voie à suivre pour désigner l'autorité « chef de file » en cas d'implication de plusieurs autorités de contrôle[171]. Ce document s'inspire de la pratique qui avait été mise en place sous le régime de la Directive, à l'initiative du Groupe de l'article 29. Le document de travail du 11 avril 2018, le WP 263, a lui-même été approuvé par l'EDPB qui a succédé au Groupe 29 le 25 mai 2018[172].

---

[167] Art. 47, § 2, m), du RGPD.

[168] Groupe 29, Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules, WP 256 rev.01, p. 3.

[169] Groupe 29, Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules, précité, p. 4.

[170] Groupe 29, Working Document setting forth a co-operation procedure for the approval of 'Binding Corporate Rules' for controllers and processors under the GDPR, 11 avril 2018, WP 263 rev.01.

[171] *Ibid.*

[172] Voy. EDPB, Endorsement 1/2018 of GDPR WP29 guidelines by the EDPB, 25 mai 2018, https://edpb.europa.eu/news/news/2018/endorsement-gdpr-wp29-guidelines-edpb_en.

Une liste des groupes/entreprises multinationales pour lesquelles des BCR ont été validées est publiée par la Commission européenne[173]. On y apprend par exemple que l'autorité chef de file pour valider les BCR élaborées par eBay était l'autorité luxembourgeoise, que celle pour Hewlett Packard était la CNIL et que celle pour ING était la commission néerlandaise.

46. Avant de donner son approbation, l'autorité compétente ou l'autorité « BCR lead » doit transmettre le dossier pour avis au Comité européen de la protection des données[174]. Cela permet de garantir la cohérence de l'application du RGPD dans l'ensemble de l'Union européenne[175].

47. On signalera, pour clôturer ce point, que le RGPD stipule que les validations de BCR accordées antérieurement à l'entrée en application du RGPD par une autorité de contrôle demeurent valables jusqu'à leur éventuelle modification, leur remplacement ou leur abrogation par l'autorité en question[176].

§ 4. Les nouveaux instruments de transfert : codes de conduite et certification

48. Ainsi qu'on l'a signalé en exergue de cette section portant sur les transferts de données à caractère personnel moyennant des garanties appropriées, le RGPD innove en permettant le recours à deux nouveaux mécanismes pour offrir les garanties appropriées en question : les codes de conduite et la certification.

a) Les codes de conduite[177]

49. L'acteur désireux de transférer des données à caractère personnel hors de l'Espace économique européen, peut offrir les garanties appropriées par la voie de l'adhésion à un code de conduite. Cette adhésion doit être assortie de l'engagement contraignant et exécutoire pris par le responsable du traitement ou le sous-traitant dans le pays tiers, au moyen d'instruments contractuels ou d'autres instruments juridiquement contraignants,

[173] « List of companies for which the EU BCR cooperation procedure is closed », 24 mai 2018, accessible à l'adresse http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=613841.
[174] Art. 64 du RGPD.
[175] Art. 63 du RGPD.
[176] Art. 46, § 5, du RGPD.
[177] Art. 46, § 2, e), du RGPD.

d'appliquer les garanties appropriées contenues dans ce code de conduite, y compris en ce qui concerne les droits des personnes concernées[178].

Les codes de conduite peuvent être élaborés par des associations ou des organismes représentant des catégories de responsables de traitement ou de sous-traitants[179].

Ils doivent être approuvés et publiés par une autorité de contrôle qui prend seule la décision (pour les codes qui ne concernent que des activités de traitement limitées à un État membre[180]) ou après application du mécanisme de cohérence impliquant de recueillir l'avis du Comité européen de la protection des données (pour les codes de conduite qui concernent des activités de traitement menées dans plusieurs États membres[181]). La Commission peut décider, par voie d'actes d'exécution, qu'un code de conduite approuvé qui lui a été soumis après application du mécanisme de cohérence, sera d'application générale au sein de l'Union[182].

b) La certification[183]

50. L'acteur désireux de transférer des données à caractère personnel hors de l'Espace économique européen peut également offrir les garanties appropriées requises en se soumettant à un mécanisme de certification. Pour ouvrir la voie aux transferts internationaux, la certification doit avoir été délivrée par un organisme de certification[184] ou par une autorité de contrôle, sur la base des critères approuvés par cette autorité de contrôle ou par le CEPD. Lorsque les critères ont été approuvés par le CEPD, cela peut donner lieu à une certification commune, le label européen de protection des données[185]. La certification permet donc de démontrer que des responsables du traitement ou des sous-traitants qui sont établis à l'étranger et ne sont pas soumis au RGPD fournissent des garanties appropriées dans le cadre des transferts de données à caractère personnel vers eux[186].

Tout comme pour l'adhésion à un code de conduite, ce mécanisme de transfert des données hors de l'UE peut se révéler très intéressant car une fois la certification obtenue, les flux de données peuvent se réaliser librement, sans nécessiter d'autorisation supplémentaire.

---

178 *Ibid.* et art. 40, § 3, du RGPD.

179 Art. 40, § 2, du RGPD. P. Van Den Bulck, « Transferts de données personnelles vers des pays tiers », *op. cit.*, p. 229.

180 Art. 40, §§ 5 et 6, du RGPD.

181 Art. 40, § 7, du RGPD.

182 Art. 40, §§ 8 et 9, du RGPD.

183 Art. 46, § 2, f), du RGPD.

184 Ces organismes sont visés à l'article 43 du RGPD.

185 Art. 42, § 5, du RGPD

186 Art. 42, § 2, du RGPD.

La certification doit toutefois s'accompagner de l'engagement contraignant et exécutoire pris par le responsable du traitement ou le sous-traitant dans le pays tiers d'appliquer les garanties appropriées, y compris en ce qui concerne les droits des personnes concernées[187].

§ 5. Les instruments spécifiques aux autorités ou organismes publics

51. Le RGPD a prévu des mécanismes spécifiques pour permettre les transferts des données à caractère personnel entre les autorités ou organismes publics de part et d'autre des frontières de l'UE ainsi que les transferts effectués par des autorités ou des organismes publics de l'UE avec des organisations internationales exerçant des missions ou fonctions correspondantes[188].

Des transferts peuvent ainsi être effectués par des autorités publiques ou des organismes publics avec des autorités publiques ou des organismes publics dans des pays tiers ou avec des organisations internationales, sur la base d'un instrument juridiquement contraignant et exécutoire fournissant les garanties appropriées[189]. Il s'agit de « dispositions à intégrer dans des arrangements administratifs, telles qu'un protocole d'accord »[190]. Cet arrangement administratif contraignant doit prévoir des droits opposables et des voies de droit effectives pour les personnes concernées[191]. Dans ce cas, il n'est pas nécessaire de solliciter une autorisation particulière d'une autorité de contrôle.

Par contre, l'autorisation de l'autorité de contrôle compétente devra être obtenue lorsque les garanties appropriées prévoyant des droits opposables et effectifs pour les personnes concernées sont intégrées dans des arrangements administratifs qui ne sont pas juridiquement contraignants[192].

SECTION 3. – Les exceptions (art. 49 du RGPD)

52. Si le pays destinataire n'offre pas un niveau de protection adéquat, et dans les cas où le recours à des garanties appropriées ne serait pas indiqué, certains transferts peuvent néanmoins avoir lieu dans certaines

187 Art. 46, § 2, f), du RGPD.
188 Art. 46, § 2, a) ; § 3, b), et considérant n° 108 du RGPD.
189 Art. 46, § 2, a), du RGPD.
190 Considérant n° 108 du RGPD.
191 Art. 46, § 1er, du RGPD.
192 Art. 46, § 3, b), et considérant n° 108 du RGPD.

circonstances limitativement énumérées par le RGPD[193]. Ces circonstances correspondent, à quelques nuances près, aux exceptions prévues par la Directive en son article 26, § 1er. Les transferts de données à caractère personnel basés sur ces exceptions ne requièrent aucune autorisation de la part d'une autorité de contrôle. Il est dès lors clair que transférer des données hors de l'Union européenne en s'appuyant sur ces dérogations (sans donc offrir de protection adéquate ou appropriée) conduit à un risque accru pour les droits et libertés des personnes concernées[194]. Cela explique l'approche restrictive qui est réservée à ces dérogations, en ligne avec les principes de droit européen[195].

Le Groupe de l'article 29 avait émis en 2005 un avis d'interprétation concernant la portée et la signification de ces exceptions, aux fins notamment d'une application uniforme de ces dispositions dans l'Union[196]. S'appuyant sur ce texte, le CEPD a adopté, le premier jour de son entrée en fonction, soit le 25 mai 2018, des lignes directrices relatives aux exceptions prévues à l'article 49 du RGPD[197].

Nous présentons ci-dessous les recommandations générales découlant de ce dernier document concernant le recours aux dérogations avant de les examiner et de les commenter une à une.

§ 1. Recommandations générales

a) Préservation des droits fondamentaux des personnes concernées

53. En tout état de cause, le recours à une des dérogations listées à l'article 49 ne doit jamais créer une situation dans laquelle les droits fondamentaux des personnes concernées par les données transférées pourraient être violés[198].

---

[193] Art. 49 du RGPD.

[194] CEPD, Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679, 25 mai 2018, p. 4.

[195] Groupe 29, Document de travail relatif à une interprétation commune des dispositions de l'article 26, paragraphe 1, de la directive 95/46/CE adopté le 25 novembre 2005, WP 114, pt 1.3. Voy. *infra*, pt e.

[196] Groupe 29, Document de travail relatif à une interprétation commune des dispositions de l'article 26, paragraphe 1, de la directive 95/46/CE adopté le 25 novembre 2005, WP 114.

[197] CEPD, Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679, 25 mai 2018.

[198] CEPD, Guidelines 2/2016, p. 3 ; Document de travail sur la surveillance des communications électroniques à des fins de renseignement et de sécurité nationale, WP 228, 5 décembre 2014, p. 39.

b) Respect des autres dispositions du RGPD

54. Le CEPD rappelle que ces dérogations ne doivent pas s'appliquer séparément des autres dispositions du RGPD[199]. Tout comme un transfert fondé sur l'adéquation dans le pays tiers ou sur l'offre de garanties appropriées doit respecter les principes de loyauté, finalité, proportionnalité, etc., un transfert fondé sur une des dérogations de l'article 49 du RGPD doit aussi respecter ces principes de base.

Le Comité propose de pratiquer un test en deux étapes face à des transferts de données à caractère personnel : il faut d'abord vérifier que ces transferts aient une base légale et répondent à toutes les conditions d'un traitement et ensuite il faut que ces transferts respectent le chapitre V du RGPD consacré aux transferts internationaux de données[200].

c) Application subsidiaire

55. Comme nous l'avons expliqué en introduction du chapitre 3 de la présente contribution[201], le recours à l'une des dérogations pour fonder un transfert international ne doit être envisagé qu'en dernière hypothèse par le responsable du traitement, lorsque le pays tiers n'offre pas une protection adéquate et lorsqu'il s'avère impossible en pratique d'obtenir des garanties appropriées via des clauses contractuelles, des BCR ou d'autres mécanismes[202].

d) Transferts occasionnels et non répétitifs

56. Les dérogations concernent en particulier des transferts pour lesquels les risques pour la personne concernée sont relativement faibles ou des situations dans lesquelles d'autres intérêts priment le droit de la personne à la protection des données. De manière générale, le CEPD a rappelé que ces dérogations visent à s'appliquer pour des transferts ponctuels de données. Le terme « occasionnel » est repris dans le considérant n° 111. Les transferts visés peuvent donc se produire « *more than once* » mais pas de façon régulière[203]. *A contrario*, les transferts de données personnelles qui pourraient être qualifiés de répétés, massifs ou structurels doivent dans toute la mesure du possible, et justement en raison de ces caractéristiques,

199 WP 114, p. 9.
200 CEPD, Guidelines 2/2016, p. 3.
201 Voy. *supra*, n° 8.
202 CEPD, Guidelines 2/2016, p. 4.
203 *Ibid.*

être encadrés de garanties appropriées[204]. Le cas, par exemple d'un transfert de données survenant régulièrement dans le contexte d'une relation stable entre l'exportateur des données et un importateur ciblé peut être qualifié de systématique et répété et ne peut donc passer pour occasionnel. Il en est de même lorsque l'importateur des données dispose d'un accès direct à une base de données, sur une base générale[205].

Aux termes du considérant n° 111, l'insistance sur le caractère occasionnel du transfert n'est que réservée aux transferts réalisés dans le cadre d'un contrat ou d'une action en justice[206]. Les lignes directrices du CEPD sont cependant venues clarifier que pour les autres exceptions – le consentement explicite, le motif important d'intérêt public, l'intérêt vital et le registre public – le transfert de données ne peut contredire « *the very nature of the derogations as being exceptions from the rule […]* »[207]. Le fait même qu'il s'agisse de dérogations devrait donc conduire à ce que les cas d'application demeurent exceptionnels et non pas généralisés. Ils ne peuvent devenir « la règle » dans la pratique mais doivent être réservés à des situations spécifiques[208].

e) Interprétation stricte

57. Enfin, le CEPD a souligné qu'en tout état de cause, ces exceptions doivent être interprétées de manière restrictive[209].

§ 2. Les dérogations

a) « La personne concernée a donné son consentement explicite au transfert envisagé, après avoir été informée des risques que ce transfert pouvait comporter pour elle en raison de l'absence de décision d'adéquation et de garanties appropriées »[210]

58. Ici, le consentement de la personne concernée devra satisfaire aux conditions posées par sa définition, à savoir celles d'une manifestation de volonté, libre, spécifique, éclairée et univoque au travers d'une déclaration

[204] CEPD, Guidelines 2/2016, pp. 4-5 ; WP 114, pt 1.3 « Recommandations sur l'utilisation respective des différentes bases juridiques offertes par la Directive pour les transferts internationaux de données ».
[205] CEPD, Guidelines 2/2016, p. 4.
[206] Soit des exceptions prévues à l'article 49, § 1er, b), c) et e).
[207] CEPD, Guidelines 2/2016, p. 5.
[208] CEPD, Guidelines 2/2016, p. 11.
[209] CEPD, Guidelines 2/2016, p. 4.
[210] Art. 49, § 1er, a), du RGPD.

ou d'un acte positif clair[211]. Les explications formulées dans la contribution de cet ouvrage dédiée aux « Principes relatifs au traitement des données à caractère personnel et à sa licéité » concernant le consentement des personnes concernées comme fondement légitime d'un traitement sont également valables ici[212]. Certaines spécificités apparaissent toutefois en présence de flux transfrontières de données. Elles sont abordées dans les paragraphes qui suivent.

59. Le consentement au transfert de données doit être *explicite*, ce qui est plus exigeant que pour un consentement au traitement en général tel qu'évoqué ci-dessus, et plus exigeant que le consentement indubitable qu'exigeait auparavant la Directive. D'après le Comité européen de la protection des données, c'est dans des situations présentant des risques particuliers en termes de protection des données qu'un tel consentement explicite est requis (comme dans le cas de données sensibles, par exemple) car ces situations demandent un haut niveau de contrôle individuel sur les données[213].

60. Le consentement doit être donné *librement* par la personne concernée, ce qui signifie que certaines situations, telles que celle où il existe un lien de subordination entre la personne concernée et le responsable de traitement, ne permettront pas l'obtention d'un consentement libre. À titre d'illustration, l'EDPS a été amené à traiter d'une plainte à propos de la procédure d'enregistrement à une conférence internationale organisée par une institution européenne. Les participants étaient tenus d'envoyer une copie scannée de leur carte d'identité ou passeport, copie qui était ensuite transmise aux autorités du pays hôte, en se basant sur le consentement des personnes concernées. L'EDPS a conclu que les consentements ne pouvaient être considérés comme ayant été donnés librement, étant donné qu'il n'y avait pas moyen de s'inscrire à la conférence sans donner son consentement au transfert des données aux autorités[214].

61. Le consentement doit être donné *spécifiquement* pour un transfert ou une catégorie de transferts de données. Cette exigence empêche de baser des transferts sur un consentement au traitement des données qui n'envisageait pas ces transferts (ce qui soulève aussi un problème sur le

[211] Art. 4.11 du RGPD. Voy. égal. les conditions développées à l'article 7 du RGPD.

[212] Voy. égal. Groupe 29, *Guidelines on consent under Regulation 2016/679*, 28 November 2017, last revised and adopted on 10 April 2018, WP 259 rev. 01. Ces lignes directrices ont été approuvées par le CEPD.

[213] CEPD, Guidelines 2/2016, p. 6.

[214] EDPS, Décision du 10 avril 2018, Newsletter n° 60, https://edps.europa.eu/press-publications/publications/newsletters/newsletter-7_en#dataprot.

plan de la transparence évoqué ci-après). C'est le cas par exemple lors du rachat d'une entreprise européenne par une autre située en dehors de l'UE à qui l'on compte transférer les données des clients de la première entité. Le consentement donné par les clients pour le traitement de leurs données dans le cadre de l'achat de biens ou de services ne pourra couvrir le transfert survenant plus tard, non envisagé à l'époque du recueil des consentements. Les personnes concernées devront donc redonner leur consentement à ce transfert spécifique[215].

62. Enfin, le consentement doit être *éclairé*, à savoir qu'il doit être satisfait à une obligation de transparence quant aux circonstances particulières du transfert (finalité, identité du/des destinataires, possibilité de retirer le consentement, utilisation ultérieure)[216]. Cette exigence est devenue particulièrement lourde dans le RGPD étant donné qu'il faut également indiquer le ou les pays destinataires des données et le fait que ces pays n'offrent pas de protection adéquate ainsi que les risques pour la personne concernée découlant de l'absence de protection adéquate et de garanties appropriées[217]. Le CEPD signale que ces informations pourraient à l'avenir être présentées sous une forme standardisée indiquant notamment si le pays destinataire dispose ou non d'une autorité de contrôle, si des principes de protection existent ou non et si des droits peuvent y être exercés ou non[218].

63. En conclusion, le CEPD estime que le RGPD a mis la barre particulièrement haut pour valider le recours au consentement des personnes concernées dans le cadre des transferts internationaux de données. Tenant compte en outre du fait que le consentement est rétractable à tout moment, le CEPD en conclut que le consentement ne représentera peut-être plus à l'avenir une solution praticable et durable pour valider les transferts de données vers des pays tiers[219].

64. On notera que les auteurs du RGPD ont exclu le recours au consentement pour valider les transferts devant intervenir dans le cadre des activités des autorités publiques dans l'exercice de leurs prérogatives de puissance publique[220].

---

[215] Exemple donné par le Comité européen de protection des données (CEPD, Guidelines 2/2016, p. 7).

[216] WP 114, pp. 12-15

[217] CEPD, Guidelines 2/2016, p. 8.

[218] *Ibid.*

[219] *Ibid.*

[220] Art. 49, § 3, du RGPD.

b) et c) « Le transfert est nécessaire à l'exécution d'un contrat entre la personne concernée et le responsable du traitement ou à la mise en œuvre de mesures précontractuelles prises à la demande de la personne concernée »[221] ou « le transfert est nécessaire à la conclusion ou à l'exécution d'un contrat conclu dans l'intérêt de la personne concernée entre le responsable du traitement et une autre personne physique ou morale »[222]

65. Ces deux dérogations appellent des interprétations communes. Tout d'abord, elles comportent toutes deux une exigence de « *nécessité* » pour que le transfert ait lieu. Dans les deux cas, ce critère de nécessité exigera un lien étroit et important entre la personne concernée et la finalité du contrat conclu ou à conclure.

Le Groupe de l'article 29[223] tout comme le CEPD[224] ont par exemple considéré que les transferts de données relatives aux salariés d'une filiale vers la société mère aux fins de centralisation des activités de gestion des ressources humaines ne pouvaient pas être considérés comme nécessaires à l'exécution du contrat de travail entre le salarié et le responsable de traitement. En effet selon le Groupe de l'article 29, une telle interprétation serait excessive « puisqu'il n'y a pas de lien direct et objectif entre l'exécution d'un contrat de travail et un tel transfert de données ». De même les transferts de données concernant des salariés par l'employeur responsable de traitement à des prestataires de services établis en dehors de l'Union dans le cadre d'un contrat de sous-traitance de gestion des salaires ne peuvent pas être considérés comme étant « dans l'intérêt des personnes concernées », en l'absence d'un lien étroit entre le salarié et le contrat de sous-traitance souscrit par le responsable de traitement. Un tel cas de figure devrait dès lors s'appuyer sur des garanties suffisantes, telles que des clauses contractuelles appropriées. En revanche, le Groupe de l'article 29 et le CEPD considèrent par exemple que les transferts par des agences de voyage de données personnelles relatives à leurs clients à des hôtels ou autres partenaires commerciaux à l'étranger en vue de l'organisation d'un séjour constituent bien des transferts nécessaires en vue de la conclusion d'un contrat[225].

66. Par ailleurs, les données à caractère personnel ne peuvent être transférées sur la base de cette dérogation que si le transfert est occasionnel[226].

---

221 Art. 49, § 1er, b), du RGP.
222 Art. 49, § 1er, c), du RGPD.
223 WP 114, pp. 16-17.
224 CEPD, Guidelines 2/2016, pp. 8-10.
225 WP 114, pp. 16-17 ; CEPD, Guidelines 2/2016, p. 9.
226 Voy. *supra*, n° 56.

C'est le cas par exemple des transferts de données à caractère personnel occasionnés lorsqu'une banque européenne exécute la demande de son client d'effectuer un paiement à une banque située hors UE à condition que ce transfert de données ne se fasse pas dans le cadre d'une relation de coopération stable entre les deux banques[227].

67. On notera qu'aux termes de l'article 49, § 3, du RGPD, ces deux dérogations liées au contrat ne sont pas applicables aux activités des autorités publiques dans l'exercice de leurs prérogatives de puissance publique.

d) « Le transfert est nécessaire pour des motifs importants d'intérêt public »[228]

68. La formulation de cette dérogation est quelque peu changée par rapport à celle de la Directive, même si l'objet de cette dérogation est resté le même. Les lignes directrices du CEPD font d'ailleurs référence à l'ancienne formulation lorsqu'elles disent : « *This derogation, usually referred to as the 'important public interest derogation', is very similar to the provision contained in Directive 95/46/EC […]* »[229]. L'adjectif « important » se rattache en fait à l'intérêt public plutôt qu'aux motifs.

69. Le considérant n° 112 du RGPD donne plusieurs exemples de transferts de données entrant dans cette exception. Il cite ainsi les cas « d'échange international de données entre autorités de la concurrence, administrations fiscales ou douanières, entre autorités de surveillance financière, entre services chargés des questions de sécurité sociale ou relatives à la santé publique, par exemple aux fins de la recherche des contacts des personnes atteintes de maladies contagieuses ou en vue de réduire et/ou d'éliminer le dopage dans le sport ».

70. La notion d'« intérêt public important » doit être entendue restrictivement. Le CEPD a notamment rappelé que les intérêts publics, fussent-ils « importants », de l'État tiers destinataire ne peuvent servir de fondement à l'utilisation de cette dérogation pour des transferts en provenance de l'Union. Seuls les intérêts publics importants de l'Union européenne elle-même ou des États membres peuvent être valablement pris en compte[230].

---

227 CEPD, Guidelines 2/2016, pp. 9-10.

228 Art. 49, § 1er, d), du RGPD.

229 CEPD, Guidelines 2/2016, p. 10.

230 Art. 49, § 4, du RGPD. CEPD, Guidelines 2/2016, p. 10. Voy. égal. Groupe 29, Avis n° 6/2002 sur la transmission par les compagnies aériennes d'informations relatives aux passagers et aux membres d'équipage et d'autres données aux États Unis, adopté le 24 août 2002, WP 66.

71. L'existence d'un accord ou traité international poursuivant certain objectif important auquel l'État européen impliqué dans un transfert de données est partie peut être un indicateur de l'existence d'un intérêt public aux termes de l'article 49, § 1, d[231]. Toutefois on se gardera de valider systématiquement tous les transferts de données effectués en exécution d'accords internationaux, sans plus veiller à entourer les données d'une certaine protection.

Il nous semble plutôt que cette dérogation de sauvegarde d'un intérêt public important visait davantage à ne pas remettre en question les accords internationaux existants au moment de la transposition de la directive 95/46/CE dans les droits des États membre. Il nous semble dès lors qu'elle ne peut pas être entendue comme conférant une exception sans conditions aux accords internationaux signés par un État membre et prévoyant des transferts. Une obligation de diligence quant au sort réservé aux données transférées s'applique à cet État lors de négociations de tels accords et oblige l'État à s'assurer que les transferts, d'une part, mais également les traitements ultérieurs d'autre part, dans le pays destinataire soient soumis à des garanties suffisantes de protection.

C'est aussi l'avis exprimé par la Commission belge de la Protection de la Vie Privée concernant des transferts de données vers le Royaume du Maroc dans le cadre d'un accord de coopération policière et judiciaire. Si elle a effectivement estimé que « de par l'existence de l'Accord de coopération du 6 mai 1999 relatif à la lutte contre la criminalité organisée …, le transfert de données à caractère personnel peut s'effectuer vers le Maroc du fait qu'il est « rendu juridiquement obligatoire pour la sauvegarde d'un intérêt public important » (art. 22, § 1er, 4° de la LVP) ; … certaines garanties supplémentaires devraient être prévues afin que les personnes concernées puissent continuer à bénéficier des droits et garanties fondamentaux reconnus à l'égard des traitements de leurs données en Belgique, une fois celles-ci transférées au Maroc »[232].

Autrement dit, la dérogation pour « sauvegarde d'un intérêt public important » pour les accords internationaux ne peut être assimilée à une dérogation comme les autres. Elle permet une certaine marge de manœuvre aux États membres dans leurs négociations avec des États tiers destinataires qui n'offrent pas de protection adéquate, mais ne peut être utilisée pour échapper totalement aux obligations positives de l'État au

[231] CEPD, Guidelines 2/2016, p. 10.

[232] Commission (belge) de la protection de la vie privée, avis n° 22/2009 du 2 septembre 2009 relatif à la compatibilité de la loi marocaine avec la loi vie privée dans le cadre de la procédure de ratification de l'Accord de coopération du 6 mai 1999 entre le Royaume de Belgique et le Royaume du Maroc relatif à la lutte contre la criminalité organisée.

titre de l'article 8 de la CEDH d'offrir certaines garanties de protection aux données transférées.

e) « Le transfert est nécessaire à la constatation, à l'exercice ou à la défense de droits en justice »[233]

72. Aux termes du considérant n° 111 du RGPD, il y a lieu d'autoriser le transfert occasionnel de données qui est nécessaire dans le cadre d'un contrat ou d'une action en justice, « qu'il s'agisse d'une procédure judiciaire, administrative ou extrajudiciaire, y compris de procédures devant des organismes de régulation »[234].

Selon les lignes directrices du CEPD, cette dérogation est soumise à une interprétation stricte et son application est réservée à des cas particuliers. Autrement dit, elle ne saurait être utilisée pour des transferts massifs ou réguliers de données. Par ailleurs, il faut qu'il y ait une « connexion réelle et substantielle » entre le transfert des données en question et la nécessité d'exercice d'un droit en justice[235].

f) « Le transfert est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'autres personnes, lorsque la personne concernée se trouve dans l'incapacité physique ou juridique de donner son consentement »[236]

73. Cette dérogation vise les situations d'urgences médicales où la personne concernée se trouve à l'étranger, dans l'impossibilité de consentir valablement au transfert, et où le transfert des données est considéré comme indispensable à l'établissement d'un diagnostic vital ou à l'administration de soins[237]. Le RGPD ne limite pas cette dérogation à l'intégrité physique de la personne concernée mais permet de prendre également en compte l'intégrité mentale de l'individu[238].

Cette hypothèse couvre désormais, à la différence de la Directive, l'intérêt vital de personnes autres que la personne concernée.

L'exception ne peut pas être utilisée pour justifier les transferts de données médicales hors de l'UE si le but du transfert n'est pas de traiter le cas particulier de la personne concernée ou celui d'une autre personne. Ainsi, si le transfert vise à alimenter une recherche scientifique d'ordre général

233 Art. 49, § 1er, e), du RGPD.

234 Pour les détails sur les différentes natures de procédures couvertes par cette dérogation, voy. CEPD, Guidelines 2/2016, pp. 11-12.

235 CEPD, Guidelines 2/2016, p. 12.

236 Art. 49, § 1er, f), du RGPD.

237 CEPD, Guidelines 2/2016, p. 12.

238 CEPD, Guidelines 2/2016, p. 13.

n'étant pas appelée à apporter des résultats avant un certain temps, on ne pourra s'appuyer sur cette dérogation pour justifier le partage des données au-delà des frontières[239].

> **g) « Le transfert a lieu au départ d'un registre qui, conformément au droit de l'Union ou au droit d'un État membre, est destiné à fournir des 'informations au public et est ouvert à la consultation du public en général ou de toute personne justifiant d'un intérêt légitime, mais uniquement dans la mesure où les conditions prévues pour la consultation dans le droit de l'Union ou le droit de l'État membre sont remplies dans le cas d'espèce »**[240]

74. Cette dérogation vise à offrir la possibilité à toute personne située à l'étranger et y ayant un intérêt légitime d'obtenir le transfert de données à caractère personnel issues d'un registre librement consultable dans un État membre[241].

Si le registre est public dans un État membre, des personnes établies dans des pays tiers doivent pouvoir y avoir y accès. Cette liberté de transfert est toutefois limitée. Elle ne peut en aucun cas servir de fondement à des transferts portant sur la totalité des données ni sur des catégories de données contenues dans le registre public. En outre, pour les registres publics qui n'ont vocation à être consultés que par les personnes qui ont un intérêt légitime, le transfert ne doit alors se faire qu'à la demande de ces personnes ou lorsqu'elles en sont les destinataires[242].

§ 3. Exception au nom des intérêts légitimes impérieux du responsable du traitement

75. Le RGPD innove en ajoutant une hypothèse à la liste des situations permettant de déroger à l'exigence de protection adéquate ou de garanties appropriées. Cette exception entièrement nouvelle et passablement interpellante ne doit être invoquée que lorsque l'on ne se trouve pas en présence d'un pays de destination ou d'une organisation internationale assurant une protection jugée adéquate ni en présence de garanties appropriées telles des clauses contractuelles ou des BCR. Il faut de plus qu'aucune des dérogations présentées ci-dessus ne trouve à s'appliquer. Dans de tels cas, il reste une hypothèse justifiant encore des transferts de données à caractère personnel. Il s'agit des cas dans lesquels un transfert

239 *Ibid.*
240 Art. 49, § 1er, g), du RGPD.
241 CEPD, Guidelines 2/2016, p. 13.
242 Art. 49, § 2, du RGPD.

de données vers un pays tiers ou à une organisation internationale est « nécessaire aux fins des intérêts légitimes impérieux poursuivis par le responsable du traitement sur lesquels prévalent les intérêts ou les droits et libertés de la personne concernée »[243].

Toutefois, cette exception est conditionnée par des exigences très strictes qui font douter de sa possibilité d'application large. Ainsi, cette exception ne pourra jouer que pour les transferts sans caractère répétitif, qui ne touchent qu'un nombre limité de personnes et qui sont nécessaires pour les intérêts légitimes impérieux du responsable du traitement sur lesquels ne prévalent pas les intérêts ou les droits et libertés de la personne concernée. En outre, le responsable du traitement doit avoir évalué toutes les circonstances entourant le transfert de données, en tenant compte de la nature des données, de la finalité et de la durée du traitement et de la « situation dans le pays tiers »[244]. À partir de cette évaluation, le responsable du traitement doit offrir des garanties appropriées (qui ne sont donc pas du même niveau que les garanties appropriées contenues dans des clauses contractuelles ou des BCR[245]) et informer l'autorité de contrôle et les personnes concernées du transfert et des intérêts impérieux en jeu[246].

Il semble, à la lecture du considérant n° 113, que le législateur européen ait eu notamment en tête les transferts à des fins de recherche scientifique ou historique ou à des fins statistiques, mettant en jeu le progrès des connaissances pour lequel la société a des attentes légitimes (mais qui ne relèvent pas d'un intérêt public important, sinon, ils seraient couverts par l'exception prévue à l'article 49, § 1er)...

SECTION 4. – Obligation d'information

76. On relèvera au terme de ce parcours à travers les instruments pour transférer des données à caractère personnel au-delà des frontières de l'Espace économique européen, que le RGPD a renforcé la transparence autour de ces transferts. Ainsi le responsable du traitement doit désormais spontanément fournir aux personnes concernées toutes les informations sur le fait qu'il a l'intention d'effectuer un transfert de données à caractère personnel à un destinataire dans un pays tiers ou une organisation

243 Art. 49, § 1er, al. 2, du RGPD.

244 Considérant n° 113.

245 La version anglaise échappe à cette formulation paradoxale en ne reprenant pas ici le terme « *appropriate safeguards* » qu'elle réserve à l'article 46, mais « *suitable safeguards* » qui marque bien qu'il ne s'agit pas du même niveau de garanties.

246 Art. 49, § 1er, al. 2, du RGPD.

internationale, ainsi que l'existence ou l'absence d'une décision d'adéquation rendue par la Commission européenne ou la référence aux garanties appropriées ou adaptées et les moyens d'en obtenir une copie ou l'endroit où elles ont été mises à disposition.

Conclusion

77. Les restrictions aux flux transfrontières qui ont été présentées dans le présent chapitre sont généralement considérées comme les plus strictes au niveau mondial. Pourtant, de nombreuses questions demeurent quant à l'effectivité de la protection conférée aux données transférées en dehors du territoire européen. Les moyens juridiques et pratiques d'assurer une protection effective continuent de soulever des défis fondamentaux si l'on observe l'intensification des flux liés au développement de l'Internet et du *cloud computing*. Ces nouvelles évolutions technologiques soulèvent des questions tant techniques, que juridiques et politiques.

Tout d'abord, les développements technologiques accroissent considérablement les flux réels de données, sans qu'il soit toujours possible de déterminer qui est en possession de celles-ci, qui en est responsable et où elles se trouvent stockées *in fine*. Les règles européennes actuelles en matière de transferts de données et les principes qui les sous-tendent (principe de transparence à l'égard des personnes concernées, transferts vers des États offrant une protection adéquate, interdiction de transferts ultérieurs sauf sous certaines conditions etc.) se trouvent mises à l'épreuve face à la multiplication et complexification des services de l'information. Du point de vue du débat juridique, deux logiques s'opposent. À l'approche dite *géographique* de l'Union européenne consistant à autoriser les transferts vers les pays assurant un niveau de protection *adéquat*, d'autres opposent une approche dite *organisationnelle*, reposant sur le principe *d'accountability* qui exige de l'entité d'origine de s'assurer que les données transférées continueront d'être protégées par le destinataire, quel que soit le lieu[247]. Plus généralement, ces questions juridiques relatives aux flux transfrontières de données portent en elles une dimension politique, en ce qu'elles exposent une confrontation de l'international avec le régional et posent la question d'une harmonisation à l'échelle internationale des

[247] Voy. par example Ch. KUNER, « Regulation of Transborder Data Flows under Data Protection and Privacy Law : Past, Present and Future », *TILT Law & Technology Working Paper*, No. 016/2010, October 2010, disponible ici : http://ssrn.com/abstract=1689483.

règles de protection de données comme solution juridique à la libéralisation des flux. Mais l'objectif est de taille, et les perspectives demeurent lointaines, si l'on observe les divergences persistantes entre les approches américaines, européennes et asiatiques de la question de la protection de la vie privée et des données à caractère personnel.