GROUPE DE TRAVAIL «ARTICLE 29» SUR LA PROTECTION DES DONNÉES

0836-02/10/FR
WP 179

Avis 8/2010 sur le droit applicable

Adopté le 16 décembre 2010

Le groupe de travail a été institué en vertu de l'article 29 de la directive 95/46/CE. Il s'agit d'un organe consultatif européen indépendant sur la protection des données et de la vie privée. Ses missions sont définies à l'article 30 de la directive 95/46/CE et à l'article 15 de la directive 2002/58/CE.

Le secrétariat est assuré par la direction C (Droits fondamentaux et citoyenneté de l'Union) de la direction générale de la justice de la Commission européenne, B-1049 Bruxelles, Belgique, bureau MO59 06/036.

Site web: http://ec.europa.eu/justice/policies/privacy/index_en.htm

Synthèse

Le présent avis clarifie le champ d'application de la directive 95/46/CE, et en particulier de son article 4, qui détermine quelle(s) loi(s) nationale(s) en matière de protection de données, adoptée(s) conformément à la directive, peu(ven)t s'appliquer aux traitements de données à caractère personnel. Il dégage en outre les domaines dans lesquels des améliorations sont encore possibles.

Délimiter l'application du droit de l'UE aux traitements de données à caractère personnel permet de clarifier le champ d'application de la législation européenne sur la protection des données, tant dans l'Union ou l'EEE que dans un contexte international plus large. Une bonne compréhension du droit applicable contribuera à garantir simultanément la sécurité juridique pour les responsables du traitement et un cadre clair pour les personnes concernées et les autres parties prenantes. Par ailleurs, une compréhension correcte des dispositions relatives au droit applicable devrait permettre de prévenir toute lacune dans le niveau élevé de protection des données à caractère personnel prévu par la directive 95/46/CE.

À l'article 4, paragraphe 1, point a), la référence à «un» établissement signifie que la présence d'un établissement du responsable du traitement sur le territoire d'un État membre entraîne l'applicabilité du droit de cet État, et que la présence d'autres établissements de ce même responsable sur le territoire d'autres États membres peut entraîner l'applicabilité du droit de ces États. La notion de «cadre des activités» de l'établissement est déterminante pour entraîner l'application du droit national. Elle suppose que l'*établissement* du responsable du traitement participe à des *activités* impliquant le traitement de données à caractère personnel. À cet égard, il convient de prendre en considération le degré de participation de l'établissement aux activités de traitement, la nature des activités, ainsi que la nécessité d'assurer la protection effective des données.

Pour ce qui est de la disposition de l'article 4, paragraphe 1, point c), concernant les moyens utilisés, qui peut entraîner l'application de la directive à des responsables du traitement non établis sur le territoire de l'Union ou de l'EEE, le présent avis précise qu'elle devrait s'appliquer dans les cas où il n'y a pas, dans l'Union ou l'EEE, d'établissement *susceptible d'entraîner l'application de l'article 4, paragraphe 1, point a)*, ou lorsque le traitement n'est *pas effectué dans le cadre* des activités d'un tel établissement. L'avis relève également qu'une interprétation large de la notion de «moyens» - justifiée par l'utilisation de termes non équivalents dans les différentes versions linguistiques de la directive («*equipment*» et non pas «*means*» en anglais) – peut, dans certains cas, entraîner l'application de la législation européenne sur la protection des données à un traitement qui ne présente pas de véritable lien avec l'UE ou l'EEE.

Le présent avis donne également des indications et des exemples concernant les autres dispositions de l'article 4; les obligations en matière de sécurité, résultant de la législation applicable conformément à l'article 17, paragraphe 3; la possibilité pour les autorités chargées de la protection des données d'exercer les pouvoirs dont elles sont investies pour vérifier un traitement effectué sur le territoire de l'État dont elles relèvent et intervenir à ce sujet, même si le droit applicable est celui d'un autre État membre (article 28, paragraphe 6).

L'avis suggère en outre qu'il serait utile de clarifier le libellé de la directive et d'améliorer la cohérence entre les différentes parties de l'article 4 lors de la révision du cadre général régissant la protection des données.

Dans cette optique, la simplification des règles de détermination du droit applicable consisterait à revenir au principe du pays d'origine: tous les établissements d'un même responsable du traitement dans l'UE appliqueraient la même législation (celle du lieu du principal établissement), indépendamment du territoire sur lequel ils seraient situés. Cependant, cela ne pourrait être acceptable que moyennant une harmonisation générale des législations nationales, dont les obligations en matière de sécurité.

On pourrait appliquer des critères supplémentaires lorsque le responsable du traitement est établi en dehors de l'UE, en vue de garantir l'existence d'un lien suffisant avec le territoire de l'Union et d'éviter que des responsables du traitement établis dans des pays tiers ne puissent utiliser ce dernier pour exercer des activités illégales de traitement de données. Les critères qui pourraient être envisagés dans cette optique sont, d'une part, le ciblage des personnes, entraînant l'application du droit de l'UE en matière de protection des données lorsque l'activité qui implique le traitement de données à caractère personnel cible des personnes résidant dans l'UE et, d'autre part, le critère des moyens, repris sous une forme résiduelle et limitée, qui couvrirait les cas limites (données concernant des personnes ne résidant pas dans l'UE, responsables du traitement sans lien avec l'UE) dans lesquels il existe une infrastructure de traitement de données sur le territoire de l'Union.

Le groupe de travail sur la protection des personnes à l'égard du traitement des données à caractère personnel

institué par la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 (JO L 281 du 23.11.1995, p. 31),

vu l'article 29 et l'article 30, paragraphe 1, point a), et paragraphe 3, de ladite directive,

vu son règlement intérieur,

a adopté l'avis suivant:

I. Introduction

La détermination du droit applicable aux traitements de données à caractère personnel visés par la directive 95/46/CE (ci-après la «directive» ou la «directive 95/46») est essentielle pour plusieurs raisons. Tout d'abord, parce que des dispositions relatives au droit applicable sont indispensables pour définir le champ d'application extérieur de la législation européenne sur la protection des données, c'est-à-dire pour déterminer si cette législation s'applique aux traitements de données à caractère personnel qui sont effectués, en tout ou partie, hors de l'Union européenne (UE) ou de l'Espace économique européen (EEE), mais qui présentent tout de même un lien avec le territoire de l'Union ou de l'EEE. Ensuite, parce que ces règles relatives au droit applicable définissent le champ d'application de la législation sur la protection des données à l'intérieur de l'Union ou de l'EEE, afin d'éviter les éventuels conflits et les chevauchements entre les lois nationales adoptées par les États membres de l'UE ou de l'EEE pour transposer la directive[1].

Enfin, une compréhension correcte des dispositions relatives au droit applicable devrait permettre de prévenir toute lacune dans le niveau élevé de protection des données à caractère personnel prévu par la directive 95/46.

Plusieurs dispositions de la directive, notamment ses articles 4, 17 et 28, portent sur le droit applicable. Elles définissent le droit national en matière de protection des données qui doit s'appliquer en vertu de la directive, ainsi que l'autorité chargée de veiller à sa bonne application. Il importe de ne pas perdre de vue qu'il existe une interaction entre droit matériel et compétence judiciaire. Cet aspect est examiné plus en détail ci-après.

Il a été signalé que la transposition et l'interprétation des dispositions de la directive relatives au droit applicable sont loin d'être uniformes dans l'Union européenne. Dans son «Premier rapport sur la mise en œuvre de la directive relative à la protection des données», la Commission soulignait en effet que la mise en œuvre de l'article 4 de la directive «pos[ait] problème dans plusieurs cas, avec pour résultat l'apparition possible du type de conflit de lois que cet article cherche justement à éviter»[2]. Selon l'annexe technique du rapport, qui présente une analyse détaillée de plusieurs dispositions nationales, cette transposition insuffisante pourrait en partie s'expliquer par la complexité même de l'article 4.

De même, une étude financée par la Commission européenne[3] souligne l'ambiguïté et la mise en œuvre inégale des règles de la directive concernant le droit applicable, et conclut qu'il «est absolument indispensable d'améliorer, de clarifier et de préciser les règles relatives au droit applicable».

---

1 La directive 95/46/CE s'applique également à la Norvège, à l'Islande et au Liechtenstein (États membres de l'Association européenne de libre-échange ou AELE) en vertu de l'accord EEE [voir la décision du Comité mixte de l'EEE n° 83/1999 du 25 juin 1999 modifiant le protocole 37 et l'annexe XI (Services de télécommunications) de l'accord EEE; JO L 296 du 23.11.2000, p. 41].

2 Premier rapport sur la mise en œuvre de la directive relative à la protection des données (95/46/CE), mai 2003, p. 17, accessible à partir de l'adresse suivante: http://ec.europa.eu/justice/policies/privacy/lawreport/report_en.htm

3 «Étude comparative sur les différentes approches des nouveaux défis en matière de protection de la vie privée, en particulier à la lumière des évolutions technologiques», janvier 2010, disponible sur l'internet à l'adresse suivante: http://ec.europa.eu/justice/policies/privacy/studies/index_en.htm

Dans une communication plus récente intitulée «Une approche globale de la protection des données à caractère personnel dans l'Union européenne»[4] , la Commission indique qu'elle «examinera la manière dont les dispositions existantes sur le droit applicable pourraient être révisées et clarifiées, notamment les critères actuels de détermination du droit applicable, en vue d'améliorer la sécurité juridique, de clarifier quel est l'État membre responsable de l'application des règles en matière de protection des données et, en définitive, d'assurer le même niveau de protection à tous les résidents de l'Union concernés, indépendamment du lieu d'établissement du responsable du traitement».

La complexité des questions liées au droit applicable s'accentue aussi du fait de la mondialisation accrue et du développement des nouvelles technologies: les entreprises sont de plus en plus amenées à exercer leur activité dans plusieurs pays et à fournir services et assistance 24 heures sur 24; l'internet facilite la prestation de services à distance ainsi que la collecte et le partage de données à caractère personnel dans un environnement virtuel; l'informatique dématérialisée («cloud computing») rend difficile la localisation des données et de l'équipement utilisé.

Il est donc essentiel que tous les acteurs publics et privés qui participent à l'application de la directive et des législations nationales sur la protection des données comprennent bien le sens exact des dispositions de la directive régissant le droit applicable.

C'est pourquoi le groupe de travail a décidé d'apporter des éclaircissements sur certaines dispositions essentielles de la directive et de se pencher sur la notion de droit applicable, comme il l'avait déjà fait pour le concept de données à caractère personnel et les notions de «responsable du traitement» et de «sous-traitant»[5]. Le présent avis renverra en outre aux autres documents et avis dans lesquels le groupe a abordé la question du droit applicable, lorsqu'elle se posera sous l'angle des aspects spécifiques couverts par ces documents[6].

L'objectif ultime du groupe de travail étant d'assurer la sécurité juridique dans l'application du droit de l'UE en matière de protection des données, il s'agit de faire en sorte que, d'une part, les personnes concernées sachent quelles sont les règles qui protègent les données à caractère personnel les concernant et que, d'autre part, les entreprises et les autres organismes publics et privés sachent quelles règles de protection des données régissent les traitements de données qu'ils effectuent.

Il est extrêmement important de préciser la notion de droit applicable, indépendamment des modifications qui pourraient être apportées à l'avenir aux dispositions actuelles de la directive. En effet, celles-ci resteront en vigueur tant qu'elles ne seront pas modifiées. Cette clarification permettra ainsi d'assurer un meilleur respect de la directive en

---

4 COM(2010) 609 final du 4.11.2010.

5 Avis 4/2007 sur le concept de données à caractère personnel (WP 136); avis 1/2010 sur les notions de «responsable du traitement» et de «sous-traitant» (WP 169). Tous les avis sont disponibles à l'adresse suivante: http://ec.europa.eu/justice/policies/privacy/workinggroup/index_en.htm

6 Il s'agit en particulier du document de travail intitulé «Application internationale du droit de l'UE en matière de protection des données au traitement des données à caractère personnel sur Internet par des sites web établis en dehors de l'UE» (WP 56), de l'avis 10/2006 sur le traitement des données à caractère personnel par la Société de télécommunications interbancaires mondiales (SWIFT) (WP 128) et de l'avis 1/2008 sur les aspects de la protection des données liés aux moteurs de recherche (WP 148).

attendant une éventuelle modification de la législation. En outre, lors des travaux préparatoires du présent avis, le groupe de travail a pu s'appuyer sur l'expérience acquise avec l'application des dispositions actuelles pour fournir au législateur des indications en vue de la révision ultérieure de la directive.

Enfin, les dispositions déterminant le droit applicable en matière de protection des données ont vocation à régir l'application de la directive dans son propre champ d'application, défini à l'article 3. Dès lors, elles interagiront fréquemment avec d'autres domaines du droit, sans les influencer au-delà du champ d'application de la directive.[7]

II. Observations générales et principaux enjeux

II.1. Bref historique: de la convention 108 à la directive 95/46/CE

En 1981, les auteurs de la convention 108, élaborée sous les auspices du Conseil de l'Europe, avaient recensé les risques posés par les problèmes de conflits de lois ou le vide juridique susceptibles de résulter de l'application de lois nationales différentes. La convention ne prévoyait cependant pas de règles particulières pour résoudre ces problèmes: le fait qu'elle crée un «noyau commun de droit matériel» était jugé suffisant pour garantir l'application des mêmes principes, malgré l'existence de réglementations différentes, et ainsi éviter des écarts de niveau de protection.

La nécessité de disposer de critères pour déterminer le droit applicable a été étudiée par la Commission européenne lors de l'élaboration de la directive sur la protection des données. Dans sa proposition initiale[8], la Commission mentionnait deux facteurs déterminants: en premier lieu, la localisation du fichier de données et, en second lieu, le lieu de résidence du responsable du traitement, si le fichier se trouve dans un pays tiers.

Lors des débats au Parlement européen et au Conseil, le critère de la localisation du fichier a été abandonné au profit de celui du lieu d'établissement du responsable du traitement. La localisation des moyens a été retenue comme second critère, pour les cas où le responsable du traitement n'est pas établi dans l'Union européenne.

Le Conseil a complété ces critères et fourni des indications complémentaires concernant la notion d'établissement. La proposition modifiée de la Commission[9]

---

7 Bien que la directive comporte des dispositions concernant la responsabilité (article 23) et les sanctions (article 24), ainsi que le mentionne le considérant 21, cela n'a en principe aucune incidence sur les principes généraux du droit civil ou pénal. Ces principes ne seraient affectés que dans la mesure nécessaire pour prévoir des sanctions en cas de violation des principes de protection des données. Dans la pratique, la transposition de la directive en droit national a donné lieu à différents scénarios, incluant ou non des sanctions pénales. Pour citer un autre exemple, bien que la directive contienne des dispositions concernant la nécessité d'obtenir le consentement des personnes concernées [voir l'article 2, point h), l'article 7, point a), et l'article 8, paragraphe 2, point a)] ou la pertinence des obligations contractuelles [voir l'article 7, point b)], elle n'évoque pas le droit des contrats (conditions de conclusion d'un contrat, droit applicable, etc.), ni les autres aspects du droit civil sortant de son champ d'application.

8 COM (1990) 314-2 du 18.7.1990: Proposition de directive du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel.

9 COM (1992) 422 final du 15.10.1992.

a ensuite précisé que le traitement doit être effectué «dans le cadre des activités d'un établissement» du responsable du traitement, et pris en compte la possibilité que ce dernier soit établi dans plusieurs États membres. Un changement capital résidait dans le fait que le principal critère de détermination du droit applicable n'était plus le lieu du principal établissement du responsable du traitement, mais *un* des lieux d'établissement de celui-ci. Les conséquences de ces modifications, s'agissant d'une application distributive, et non pas uniforme, du droit national en cas d'établissements multiples, sont décrites ci-après.

II.2. Le rôle des notions

II.2.a) Contexte et importance stratégique

Comme il a été indiqué précédemment, délimiter l'application du droit de l'UE aux traitements de données à caractère personnel permettra de clarifier le champ d'application de la législation européenne sur la protection des données, tant dans l'Union ou l'EEE que dans un contexte international plus large. Une bonne compréhension du droit applicable contribuera à garantir simultanément la sécurité juridique pour les responsables du traitement et un cadre clair pour les personnes concernées et les autres parties prenantes.

La détermination du droit applicable est étroitement liée à l'identification du responsable du traitement[10] et de son (ses) établissement(s): la principale conséquence de ce lien est la réaffirmation des responsabilités du responsable du traitement, ou de son représentant si le responsable du traitement est établi dans un pays tiers.

Ainsi qu'il sera exposé ci-après, cela ne signifie pas qu'il y aura toujours une seule législation applicable, notamment si le responsable du traitement dispose de plusieurs établissements: la situation géographique de ces derniers et la nature de leurs activités seront également déterminantes. Néanmoins, le lien évident entre le droit applicable et le responsable du traitement peut être une garantie d'efficacité et d'opposabilité, notamment lorsque le contexte rend difficile, voire impossible parfois, la localisation d'un fichier (comme cela peut être le cas avec l'informatique dématérialisée).

Des lignes directrices précises sur les règles relatives au droit applicable aideront à faire face aux nouvelles évolutions technologiques (internet, fichiers en réseau, informatique dématérialisée) et commerciales (entreprises multinationales).

II.2.b) Champ d'application du droit de l'UE et du droit national dans l'Union ou l'EEE

Les principaux critères à prendre en considération pour déterminer le droit applicable sont le lieu d'établissement du responsable du traitement et, si celui-ci se trouve en dehors de l'EEE, la localisation des moyens[11] utilisés. Il s'ensuit que ni la nationalité ou le lieu de résidence habituelle des personnes concernées, ni la

[10] Voir l'avis 1/2010 sur les notions de «responsable du traitement» et de «sous-traitant» (WP 169).

[11] Comme l'explique le point III.2.b ci-dessous, la notion d'«*equipment*» figurant dans la version anglaise de la directive est exprimée dans les autres versions linguistiques, notamment le texte en langue française, par le terme «moyens» («*means*» en anglais), d'où la nécessité de donner une interprétation large à cette notion.

localisation physique des données à caractère personnel, ne sont déterminants à cet égard[12].

Il en résulte un large champ d'application, dont les effets juridiques s'étendent au-delà du territoire de l'EEE: la directive, ainsi que les dispositions nationales qui la transposent, s'appliquent aux traitements de données à caractère personnel effectués en dehors de l'EEE (dans le cadre des activités d'un établissement du responsable du traitement situé à l'intérieur de l'EEE), de même qu'aux responsables du traitement établis en dehors de l'EEE (lorsqu'ils recourent à des moyens situés à l'intérieur de l'EEE). Les dispositions de la directive peuvent donc s'appliquer aux services revêtant une dimension internationale, tels que les moteurs de recherche, les réseaux sociaux et l'informatique dématérialisée. Ces exemples sont plus amplement développés dans la suite du document.

Lorsque des données à caractère personnel sont traitées par un responsable du traitement (X) dont l'unique établissement est situé dans l'État membre A, c'est le droit national de cet État qui s'applique à ces traitements, indépendamment du lieu où ils sont effectués.

Si X possède un autre établissement (Y) dans un État membre B, c'est le droit national de cet État membre B qui s'applique aux traitements effectués par Y, à condition qu'ils le soient dans le cadre des activités de Y. Si les traitements effectués par Y le sont dans le cadre des activités de l'établissement de X situé dans l'État membre A, c'est le droit national de cet État qui s'applique à ces traitements.

Lorsque des données à caractère personnel sont traitées par un responsable du traitement qui n'est établi dans aucun État membre, ces traitements relèvent du champ d'application du droit national de tout État membre dans lequel sont situés les moyens utilisés par le responsable aux fins de ces traitements. Ces différents scénarios sont illustrés plus loin dans le présent avis.

Ce large champ d'application a pour finalité première d'assurer que les personnes ne soient pas privées de la protection qui leur est accordée par la directive et, dans le même temps, d'éviter tout contournement de la législation.

La directive prévoit des critères permettant de déterminer:

a) si le droit européen, combiné ou non avec celui d'un pays tiers, s'applique à un traitement de données à caractère personnel; et
b) lorsque le droit européen s'applique au traitement, les États membres dont le droit national s'applique également.

Il convient par ailleurs de noter que certains traitements effectués à l'intérieur de l'Union ne relèvent pas du champ d'application de la directive, mais qu'ils peuvent entraîner l'application d'autres instruments juridiques européens, comme la décision-cadre 2008/977/JAI relative à la protection des données dans le cadre de la

[12] Voir, en ce sens, la directive 2000/31/CE relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur. La localisation du sous-traitant est un autre facteur à prendre en compte pour déterminer le droit applicable aux mesures de sécurité (article 17). Toutefois, ce critère n'est pas déterminant en soi; il complète le critère principal, celui de l'établissement du responsable du traitement.

coopération policière et judiciaire en matière pénale[13], le règlement (CE) n° 45/2001 relatif aux données à caractère personnel traitées par les institutions et organes communautaires[14], ou d'autres instruments portant sur des organismes ou des systèmes d'information particuliers de l'UE [Europol, Eurojust, système d'information Schengen (SIS), système d'information douanier (SID), etc.).[15]

II.2.c) Éviter les lacunes et les chevauchements

La définition de critères précis pour la détermination du droit applicable vise à éviter le contournement des règles nationales des États membres, ainsi que le chevauchement de ces dernières. Une ou plusieurs législations peuvent s'appliquer à un traitement, selon le nombre d'établissements du responsable du traitement et les activités de son ou ses établissements:

- si le responsable du traitement n'a qu'un établissement, une seule législation, déterminée en fonction du lieu où celui-ci est situé, s'appliquera sur l'ensemble du territoire de l'Union ou de l'EEE;[16]

- s'il dispose de plusieurs établissements, l'application des législations nationales sera répartie selon les activités de chaque établissement.

L'application des critères devrait empêcher l'application simultanée de plusieurs législations nationales à un même traitement.

II.2.d) Droit applicable et compétence judiciaire dans le cadre de la directive

En matière de protection des données, il est importe tout particulièrement de distinguer la notion de *droit applicable* (qui détermine le régime juridique régissant telle ou telle situation) de celle de *compétence judiciaire* (qui détermine généralement l'aptitude d'une juridiction nationale à statuer sur une affaire ou à faire appliquer une décision de justice). Il peut arriver que le droit applicable et la compétence judiciaire ne soient pas les mêmes pour un traitement donné.

Le champ d'application extérieur du droit de l'UE traduit la capacité de l'Union de fixer des règles destinées à protéger les intérêts fondamentaux sur son territoire. Les dispositions de la directive définissent en outre le champ d'application des législations nationales des États membres, mais elles sont sans effet sur la compétence des juridictions nationales pour statuer dans les affaires dont elles sont saisies. En revanche, elles indiquent la compétence territoriale des autorités de contrôle habilitées à appliquer et à faire appliquer le droit applicable.

---

13 Décision-cadre 2008/977/JAI du Conseil du 27 novembre 2008 relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale (JO L 350 du 30.12.2008, p. 60).

14 Règlement (CE) n° 45/2001 du Parlement européen et du Conseil du 18 décembre 2000 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données (JO L 8 du 12.1.2001, p. 1).

15 Europol: décision 2009/371/JAI du Conseil (JO L 121 du 15.5.2009, p. 37); Eurojust: décision 2002/187/JAI du Conseil (JO L 63 du 6.3.2002, p. 1), modifiée par la décision 2009/426/JAI du Conseil (JO L 138 du 4.6.2009, p. 14).

16 Sauf en ce qui concerne les mesures de sécurité, qui dépendent de la localisation d'un éventuel sous-traitant, conformément à l'article 17, paragraphe 3, de la directive.

Bien que ces deux notions, droit applicable et compétence des autorités de contrôle, coïncident dans la plupart des cas, en conséquence de quoi ce sont les autorités de l'État membre A qui font appliquer le droit de cet État membre A, la directive prévoit explicitement la possibilité qu'il en soit autrement. Ainsi, l'article 28, paragraphe 6, implique que les autorités nationales chargées de la protection des données puissent exercer leurs pouvoirs lorsque la législation en la matière d'un autre État membre s'applique à un traitement de données à caractère personnel effectué dans l'État membre dont ces autorités relèvent. Les conséquences pratiques de ce cas de figure feront l'objet d'un examen plus approfondi dans un prochain avis du groupe de travail.

Ce type de situation conduit à devoir traiter des affaires transfrontières, et souligne le besoin d'une coopération entre les autorités chargées de la protection des données, tenant compte des pouvoirs d'exécution de chaque autorité concernée. Cela montre également la nécessité que les législations nationales transposent correctement les dispositions pertinentes de la directive, cela pouvant être déterminant pour une coopération transfrontière efficace et une bonne application transfrontière de la législation.

III. Analyse des dispositions

La principale disposition concernant le droit applicable est l'article 4, qui détermine quelle(s) loi(s) nationale(s) en matière de protection de données, adoptée(s) conformément à la directive, peu(ven)t s'appliquer aux traitements de données à caractère personnel.

III.1. Responsable du traitement établi dans un ou plusieurs États membres [article 4, paragraphe 1, point a)]

L'article 4, paragraphe 1, règle en premier lieu la situation où le responsable du traitement a un ou plusieurs établissements sur le territoire de l'Union. Dans ce cas, son point a) prévoit qu'un État membre applique son droit national en matière de protection des données lorsque «*le traitement est effectué dans le cadre des activités d'un établissement du responsable du traitement sur le territoire de l'État membre; si un même responsable du traitement est établi sur le territoire de plusieurs États membres, il doit prendre les mesures nécessaires pour assurer le respect, par chacun de ses établissements, des obligations prévues par le droit national applicable*».

Il est utile de rappeler que la notion de «responsable du traitement» est définie à l'article 2, point d), de la directive. Cette définition n'est pas analysée dans le présent avis, puisque le groupe de travail l'avait déjà expliquée dans son avis sur les notions de «responsable du traitement» et de «sous-traitant»[17].

Il importe en outre de souligner que les établissements ne doivent pas nécessairement être dotés de la personnalité juridique, et que la notion d'établissement présente des liens flexibles avec la notion de contrôle. Un responsable du traitement peut avoir plusieurs établissements, de même que des responsables associés peuvent concentrer leurs activités dans un seul ou dans divers établissements. L'élément déterminant pour qu'un établissement relève de la directive est l'exercice effectif et réel d'activités dans le cadre desquelles des données à caractère personnel sont traitées.

[17] Avis 1/2010 sur les notions de «responsable du traitement» et de «sous-traitant» (WP 169).

a) «[…] un établissement du responsable du traitement sur le territoire de l'État membre […]»

La notion d'établissement n'est pas définie dans la directive. Son préambule indique toutefois que «*l'établissement sur le territoire d'un État membre suppose l'exercice effectif et réel d'une activité au moyen d'une installation stable [et] que la forme juridique retenue pour un […] établissement, qu'il s'agisse d'une simple succursale ou d'une filiale ayant la personnalité juridique, n'est pas déterminante à cet égard*» (considérant 19).

En ce qui concerne la liberté d'établissement prévue par l'article 50 du TFUE (ex-article 43 TCE), la Cour de Justice de l'Union européenne (CJUE) a considéré que pour être qualifié de stable, un établissement doit comporter «la réunion permanente des moyens humains et techniques nécessaires à des prestations de services déterminées».[18]

L'accent mis dans le préambule de la directive sur «l'exercice effectif et réel d'une activité au moyen d'une installation stable» reflète clairement la notion d'«établissement stable» évoquée par la Cour de justice au moment de l'adoption de la directive. Bien qu'il ne soit pas certain que cette interprétation et celles données ultérieurement par la CJUE concernant la liberté d'établissement prévue par l'article 50 du traité UE puissent s'appliquer intégralement aux situations visées à l'article 4 de la directive sur la protection des données, l'interprétation de la Cour dans les affaires évoquées peut néanmoins fournir des indications utiles pour l'analyse du libellé de la directive.

Cette interprétation est retenue dans les exemples suivants:

- lorsque «l'exercice effectif et réel d'une activité» a lieu dans un cabinet d'avocat, par exemple, au moyen d'une «installation stable», ce cabinet peut être qualifié d'établissement;

- un serveur ou un ordinateur n'est pas susceptible d'être qualifié d'établissement, puisqu'il s'agit simplement d'une installation technique ou d'un outil de traitement d'informations[19];

- un bureau unipersonnel peut être qualifié d'établissement pour autant qu'il ne se borne pas à représenter un responsable du traitement établi ailleurs et qu'il participe activement aux activités dans le cadre desquelles les traitements de données à caractère personnel sont effectués;

---

[18] Voir l'arrêt du 4 juillet 1985, *Berkholz* (affaire 168/84, Rec. 1985, p. 2251, point 18), ainsi que l'arrêt du 7 mai 1998, *Lease Plan Luxembourg/Belgische Staat* (C-390/96, Rec. 1998, p. I-2553). Dans cette seconde affaire, la question posée était de savoir si le serveur d'une entreprise, situé dans un pays différent de celui du prestataire, pouvait être considéré comme un établissement stable. Il s'agissait de déterminer dans quel pays la TVA devait être payée. La Cour a refusé de considérer des moyens informatiques comme un établissement virtuel [revenant ainsi à une interprétation plus «classique» de la notion d'«établissement», différente de celle retenue précédemment dans l'arrêt du 17 juillet 1997, *ARO Lease/Inspecteur der Belastingdienst Grote Ondernemingen te Amsterdam* (C-190/95, Rec. 1997 p. I-4383)].

[19] La question de savoir s'il y a tout de même lieu de les prendre en considération, par exemple en tant que «moyens», est examinée plus loin dans le texte.

- en tout état de cause, la forme juridique n'est pas déterminante: même un simple agent peut être considéré comme un établissement si sa présence dans l'État membre présente une stabilité suffisante.

Exemple nº 1: publication à l'intention des voyageurs

Une entreprise établie dans l'État membre A recueille des informations concernant les services proposés par les stations-service dans un État membre B, afin de produire une publication destinée aux voyageurs. Les informations sont recueillies par un employé qui se déplace à travers l'État membre B, où il prend des photos qu'il envoie, accompagnées de commentaires, à son employeur dans l'État membre A. Dans cet exemple, les données sont recueillies dans l'État membre B (où il n'y a pas d'«établissement») et traitées dans le cadre des activités de l'établissement situé dans l'État membre A: le droit applicable est celui de l'État membre A.

L'article 4, paragraphe 1, point a), où il est question d'*un* établissement *du responsable du traitement* sur le territoire de l'*État membre*, suscite des interrogations (sur des sujets autres que la notion d'établissement) auxquelles il convient de répondre.

Tout d'abord, la référence à «un» établissement signifie que la présence d'un établissement du responsable du traitement sur le territoire d'un État membre entraîne l'applicabilité du droit de cet État, et que la présence d'autres établissements de ce même responsable sur le territoire d'autres États membres peut entraîner l'applicabilité du droit de ces États.

Même si le principal établissement du responsable du traitement est situé dans un pays tiers, le simple fait de disposer d'un établissement dans un État membre peut entraîner l'applicabilité du droit de cet État, pour autant que les autres conditions énoncées à l'article 4, paragraphe 1, point a), soient réunies [voir point b) ci-dessous]. Cette thèse est d'ailleurs confirmée par la seconde partie de la disposition, qui prévoit explicitement que si un même responsable du traitement est établi sur le territoire de plusieurs États membres, il doit veiller à ce que chacun de ses établissements respecte le droit applicable.

b) «[…] le traitement est effectué dans le cadre des activités […]»

La directive lie l'applicabilité du droit d'un État membre en matière de protection des données à un traitement de données à caractère personnel. Le groupe de travail a déjà évoqué la notion de «traitement», à titre accessoire, dans des avis antérieurs, qui soulignaient que plusieurs opérations ou ensembles d'opérations appliquées à des données à caractère personnel peuvent se dérouler simultanément ou en différentes étapes.[20] S'agissant de la détermination du droit applicable, cela pourrait signifier que les différentes étapes d'un traitement de données à caractère personnel peuvent entraîner l'applicabilité de différentes législations.

La multiplication des législations applicables devenant dès lors un risque sérieux, il convient d'examiner la possibilité que des liens (à un niveau macro) entre les différentes activités de traitement puissent conduire à l'application d'une seule législation nationale. Pour déterminer si une ou plusieurs législations doivent s'appliquer aux différentes

[20] Voir, par exemple, l'avis 1/2010 sur les notions de «responsable du traitement» et de «sous-traitant» (WP 169).

étapes d'un traitement, il importe de garder à l'esprit le schéma global des activités de traitement: il se peut ainsi qu'un ensemble de traitements effectués dans plusieurs États membres mais ayant tous une même finalité entraîne l'application d'une seule législation nationale.

Dans ces conditions, c'est la notion de «cadre des activités», et non la localisation des données, qui est un facteur déterminant pour la définition du droit applicable.

La notion de «cadre des activités» implique que le droit applicable est non celui de l'État membre dans lequel le *responsable du traitement* est établi, mais celui de l'État dans lequel un *établissement* du responsable du traitement participe à des *activités* liées au traitement de données.

L'examen de différents scénarios peut aider à clarifier cette notion et son influence sur la détermination du droit applicable à différentes activités de traitement effectuées dans plusieurs pays.

a. Lorsqu'un responsable du traitement a un établissement en Autriche et qu'il traite des données à caractère personnel dans ce pays, dans le cadre des activités de cet établissement, le droit applicable est bien évidemment celui de l'Autriche, c'est-à-dire celui de l'État dans lequel l'établissement est situé.

b. Deuxième scénario: le responsable du traitement a un établissement en Autriche, dans le cadre des activités duquel il traite des données à caractère personnel recueillies par le biais de son site web, accessible dans plusieurs pays. Le droit applicable est toujours celui de l'Autriche, c'est-à-dire celui de l'État dans lequel l'établissement est situé, indépendamment du lieu où se trouvent les utilisateurs du site et les données.

c. Troisième scénario: le responsable du traitement est établi en Autriche et confie les traitements à un sous-traitant en Allemagne. Les traitements effectués en Allemagne le sont dans le cadre des activités du responsable du traitement en Autriche. Autrement dit, les traitements sont effectués pour les besoins et sur instruction de l'établissement autrichien. Le droit autrichien s'applique donc aux traitements effectués par le sous-traitant en Allemagne. En outre, le sous-traitant est soumis aux exigences du droit allemand concernant les mesures de sécurité qu'il est tenu de mettre en place pour les traitements[21]. Un tel cas de figure nécessiterait un contrôle coordonné de la part des autorités chargées de la protection des données en Allemagne et en Autriche.

d. Quatrième scénario: le responsable du traitement, établi en Autriche, ouvre un bureau de représentation en Italie, qui organise l'ensemble du contenu italien du site web et traite les demandes des utilisateurs italiens. Les traitements de données effectués par

[21] Selon l'article 17, paragraphe 3, de la directive 95/46/CE, le sous-traitant est soumis aux obligations définies par la législation de l'État membre dans lequel il est établi en ce qui concerne les mesures de sécurité. En cas de conflit entre les obligations matérielles définies par la législation du pays du sous-traitant et celles qui sont prévues par la législation du pays d'établissement du responsable du traitement, la législation du pays du sous-traitant prévaut (principe de la *lex loci*). Bien que le responsable du traitement reste responsable en dernier ressort, le sous-traitant doit apporter la preuve qu'il a pris toutes les mesures requises par son contrat avec le responsable du traitement et respecté les obligations qui lui incombent en matière de sécurité, telles que définies par la législation de l'État membre dans lequel il est établi (voir le point III.5 ci-après pour plus de détails).

le bureau italien le sont dans le cadre des activités de l'établissement italien, si bien que c'est le droit italien qui s'applique à ces traitements.

On ne peut tirer des conclusions sur le droit applicable qu'en ayant une compréhension précise de la notion «dans le cadre des activités». Les éléments à prendre en considération aux fins de cette analyse sont exposés ci-après.

Le degré de participation du ou des établissements aux activités dans le cadre desquelles des données à caractère personnel sont traitées revêt une importance capitale. Il s'agit ici d'établir «qui fait quoi», c'est-à-dire quelles activités sont exercées par quel établissement, afin de pouvoir déterminer si l'établissement est l'élément qui entraîne l'application du droit national en matière de protection des données. Lorsqu'un établissement traite des données à caractère personnel dans le cadre de ses propres activités, le droit applicable est celui de l'État membre dans lequel il est situé, tandis que lorsqu'il traite de telles données dans le cadre des activités d'un autre établissement, le droit applicable est celui de l'État membre dans lequel cet autre établissement est situé.

Bien qu'il s'agisse d'un élément secondaire, la nature des activités des établissements facilite la détermination du droit applicable à chaque établissement: la question de savoir si une activité suppose ou non un traitement de données, et quel traitement est effectué dans le cadre de quelle activité, dépend en grande partie de la nature de ces activités. Par ailleurs, le fait que divers établissements puissent prendre part à des activités complètement différentes, dans le cadre desquelles des données à caractère personnel sont traitées, aura une incidence sur le droit applicable. L'exemple n° 4 illustre ces considérations.

Il convient également de tenir compte de l'objectif général de la directive, puisque celle-ci vise à assurer une protection efficace aux personnes physiques, selon des modalités simples, réalisables et prévisibles.

Exemple n° 2: transfert de données à caractère personnel dans le cadre d'une opération d'affacturage

Une société italienne de distribution d'énergie transmet des informations concernant ses débiteurs à une banque d'investissement française en vue de l'affacturage des créances correspondantes, résultant du non-paiement de factures d'électricité. Cette transmission d'informations sur les créances suppose le transfert de données à caractère personnel concernant des clients à la banque d'investissement française, et plus précisément à sa succursale en Italie (c'est-à-dire l'établissement de la banque française en Italie).

La banque d'investissement française est responsable des traitements qui constituent le transfert, tandis que sa succursale italienne s'occupe de la gestion et du recouvrement des créances pour son compte. Les données sont traitées par le responsable en France et au sein de la succursale italienne. Le responsable français informe tous les clients italiens de l'opération décrite ci-dessus par l'intermédiaire de la succursale italienne.

La succursale italienne est un établissement au sens de la directive, et ses activités consistant à traiter des données à caractère personnel afin d'informer les clients de l'opération d'affacturage doivent respecter la législation italienne sur la protection des données. Les mesures de sécurité prises au sein de la succursale italienne doivent également satisfaire aux conditions fixées par cette législation, tandis que le responsable français doit se conformer en parallèle, en ce qui concerne les données traitées au sein de son établissement en France, aux obligations définies par la législation française en matière de sécurité. Les personnes concernées, c'est-à-dire les débiteurs, peuvent s'adresser à la succursale italienne pour exercer les droits qui leur sont reconnus par la législation italienne en matière de protection des données, notamment leurs droits d'accès, de rectification et d'effacement.

Il convient d'adopter une approche fonctionnelle pour analyser ces critères: ce sont davantage le comportement des parties et leur interaction (quel est le rôle exact de chaque établissement? Quelle activité a lieu dans le cadre de quel établissement?) que leur évaluation théorique du droit applicable qui sont déterminants.

Il y a lieu de tenir compte du degré de participation de chaque établissement aux activités dans le cadre desquelles des données à caractère personnel sont traitées. Il est donc également utile de bien comprendre la notion «dans le cadre de» dans les cas complexes, afin de dissocier les différentes activités exercées par les divers établissements d'une même entreprise situés sur le territoire de l'Union.

Exemple nº 3: collecte de données sur les clients réalisée par des magasins

Une chaîne de prêt-à-porter a son siège en Espagne et des boutiques dans toute l'Union. La collecte de données concernant les clients est effectuée dans chaque magasin, mais les données sont transférées au siège espagnol, où certaines activités liées au traitement des données sont réalisées (analyse des profils des clients, service clients, publicité ciblée).

Certaines activités, comme la prospection auprès de la clientèle européenne, sont décidées exclusivement par le siège en Espagne. Il en résulte que ces activités ont lieu dans le cadre des activités de l'établissement espagnol. C'est donc le droit espagnol qui s'y applique.

En revanche, les boutiques demeurent responsables des aspects du traitement des données à caractère personnel concernant leurs clients qui ont lieu dans le cadre de leurs activités (comme la collecte des coordonnées des clients, par exemple). Dans la mesure où ce traitement est effectué dans le cadre des activités de chaque boutique, il est soumis au droit du pays dans lequel cette dernière est établie.

Il résulte directement de cette analyse que chaque boutique doit prendre les mesures requises par sa propre législation nationale pour informer ses clients des conditions de collecte et de traitement ultérieur des données les concernant.

En cas de réclamation, les clients peuvent s'adresser directement à l'autorité chargée de la protection des données dans leur propre pays. Si la réclamation porte sur les actions de prospection réalisées dans le cadre des activités du siège espagnol, l'autorité saisie devra transmettre le dossier à son homologue espagnole.

Il est donc possible qu'un même établissement participe à divers types d'activités et que des législations nationales différentes s'appliquent aux traitements de données effectués dans le cadre de ces diverses activités. Afin d'avoir une approche prévisible et réalisable en cas d'applicabilité potentielle de plusieurs législations aux diverses activités d'un même établissement, il convient d'adopter une approche fonctionnelle, qui tienne compte du contexte juridique plus large.

Exemple nº 4: base de données centralisée sur les ressources humaines

Les situations où différentes législations peuvent s'appliquer à une même base de données sont de plus en plus fréquentes. Tel est souvent le cas dans le domaine des ressources humaines, lorsque des filiales ou des établissements situés dans plusieurs pays centralisent les informations concernant les employés dans une même base de données. Si cette pratique a généralement pour but de permettre des économies d'échelle, elle ne doit cependant pas avoir d'incidence sur les responsabilités de chaque établissement prévues par la législation locale, et ce non seulement en ce qui concerne la protection des données, mais aussi dans le domaine du droit du travail et en matière d'ordre public.

Par exemple, si des données concernant les employés d'une filiale irlandaise (pouvant être qualifiée d'établissement) sont transférées dans une base de données centralisée au Royaume-Uni, dans laquelle sont également enregistrées des informations concernant les employés de la filiale ou l'établissement britannique, deux législations différentes (irlandaise et britannique) sur la protection des données s'appliqueront.

L'application de ces deux législations nationales distinctes ne résulte pas simplement du fait que les données proviennent de deux États membres, mais plutôt du fait que le traitement des données relatives aux employés irlandais par l'établissement britannique a lieu dans le cadre des activités de l'établissement irlandais en sa qualité d'employeur.

Cet exemple témoigne que ce n'est pas le lieu où les données se trouvent ou vers lequel elles sont transférées qui détermine le droit national applicable, mais que ce sont essentiellement la nature des activités habituelles et le lieu d'exercice de celles-ci qui définissent le «cadre» dans lequel le traitement est effectué: les données concernant les ressources humaines ou les clients sont ainsi normalement soumises au droit du pays dans lequel l'activité (dans le cadre de laquelle elles sont traitées) a lieu. Cet exemple confirme également l'absence de corrélation directe entre droit applicable et compétence judiciaire, une législation nationale pouvant s'appliquer en dehors du territoire national.

En résumé, les critères utilisés pour déterminer le droit applicable jouent un rôle à différents niveaux:

- premièrement, ils permettent d'établir si le droit de l'UE en matière de protection des données s'applique ou non à un traitement;

- deuxièmement, si le droit de l'UE s'applique, ils détermineront:
  a) le droit national en matière de protection des données qui est applicable, et
  b) dans le cas d'établissements multiples dans différents États membres, le droit de quel État membre s'applique à quel traitement;

- troisièmement, les critères facilitent la détermination du droit applicable lorsque les traitements revêtent une dimension extra-européenne, comme dans l'exemple suivant, où le responsable du traitement est établi en dehors de l'EEE.

Exemple nº 5: fournisseur de services internet (FSI)

Un fournisseur de services internet (le responsable du traitement) a son siège en dehors de l'Union, par exemple au Japon. Il dispose d'antennes commerciales dans la plupart des États membres de l'UE, ainsi qu'un bureau en Irlande, chargé de tout ce qui concerne le traitement des données à caractère personnel, dont l'assistance informatique. Le responsable du traitement met en place, en Hongrie, un centre de données doté de personnel et de serveurs affectés au traitement et au stockage des données concernant les utilisateurs de ses services.

Le responsable du traitement établi au Japon possède également, dans plusieurs États membres de l'UE, d'autres établissements qui exercent des activités différentes:

- le centre de données situé en Hongrie n'intervient qu'en ce qui concerne la maintenance technique;

- les antennes commerciales du FSI organisent des campagnes générales de publicité;

- le bureau irlandais est le seul des établissements situés dans l'UE à exercer des activités dans le cadre desquelles des données à caractère personnel sont effectivement traitées (nonobstant la contribution du siège japonais).

Les activités du bureau irlandais entraînent l'application du droit de l'UE en matière de protection des données: puisque les données à caractère personnel sont traitées dans le cadre des activités du bureau irlandais, ces traitements sont soumis à la législation européenne sur la protection des données.

C'est la législation irlandaise sur la protection des données qui s'applique aux traitements effectués dans le cadre des activités du bureau irlandais, qu'ils aient lieu au Portugal, en Italie ou dans n'importe quel autre État membre.

Dès lors, dans ce cas de figure, le centre de données situé en Hongrie devrait donc se conformer à la législation irlandaise sur la protection des données pour les traitements de données à caractère personnel concernant les clients du FSI. Cela n'empêcherait toutefois pas l'application de la législation hongroise aux autres traitements de données à caractère personnel que le centre de données hongrois pourrait effectuer dans le cadre de ses propres activités, par exemple le traitement des données à caractère personnel concernant ses employés.

Pour ce qui est des antennes commerciales basées dans d'autres États membres, si leur activité se limite à l'organisation de campagnes publicitaires générales non ciblées, n'impliquant pas le traitement des données à caractère personnel des utilisateurs, les législations européennes sur la protection des données ne leur sont pas applicables. En revanche, si elles décident de procéder, dans le cadre de leurs activités, au traitement de données à caractère personnel concernant des personnes résidant dans leur pays d'établissement (envoi de publicités ciblées aux utilisateurs et à de futurs utilisateurs potentiels aux fins de leurs propres activités professionnelles, par exemple), elles doivent se conformer à la législation locale sur la protection des données.

En l'absence de lien entre les traitements de données et l'établissement irlandais (l'assistance informatique, très limitée, n'intervient pas dans le traitement de données à caractère personnel), d'autres dispositions de la directive peuvent tout de même entraîner l'application des principes de protection des données, par exemple si le responsable du traitement recourt à des moyens situés sur le territoire de l'UE. Cette éventualité est examinée au point III.3 ci-après.

III.2. Le responsable du traitement est établi en un lieu où la législation de l'État membre s'applique en vertu du droit international public [article 4, paragraphe 1, point b)]

L'article 4, paragraphe 1, point b), règle la situation, moins courante, où la législation d'un État membre en matière de protection des données s'applique lorsque «le responsable du traitement n'est pas établi sur le territoire de l'État membre mais en un lieu où sa loi nationale s'applique en vertu du droit international public».

III.2.a) «[…] le responsable du traitement n'est pas établi sur le territoire de l'État membre […]»

Pour des raisons de cohérence avec les autres dispositions de l'article 4, paragraphe 1, la première condition doit être interprétée en ce sens que le responsable du traitement ne dispose, sur le territoire de l'État membre, d'aucun établissement susceptible d'entraîner l'applicabilité de l'article 4, paragraphe 1, point a) (voir également le point III.3.a) ci-dessous). Autrement dit, en l'absence d'établissement pertinent sur le territoire de l'Union, il n'est pas possible de définir la législation nationale applicable en matière de protection des données au regard de l'article 4, paragraphe 1, point a).

III.2.b) «[…] mais en un lieu où sa loi nationale s'applique en vertu du droit international public […]»

Cependant, des critères externes issus du droit international public peuvent avoir pour effet, dans des situations particulières, d'étendre l'application d'une législation nationale sur la protection des données au-delà des frontières nationales. Il peut en être ainsi lorsque le droit international public ou des accords internationaux déterminent le droit applicable dans une ambassade ou un consulat, ou à un navire ou un aéronef. Quand le responsable du traitement est établi en l'un de ces lieux particuliers, c'est le droit international qui détermine la législation nationale applicable en matière de protection des données.

Il importe toutefois de souligner aussi qu'une législation nationale sur la protection des données peut ne pas s'appliquer aux missions étrangères ou aux organisations internationales présentes sur le territoire de l'Union dans la mesure où, en vertu du droit international, celles-ci ci sont dotées d'un statut particulier, défini dans un accord général ou dans un accord de siège, qui empêche l'application de l'article 4, paragraphe 1, point a), à leur égard.

Exemple nº 6: ambassades étrangères

L'ambassade d'un État membre de l'UE au Canada est soumise à la législation sur la protection des données de l'État membre en question, et non à celle du Canada.

Aux Pays-Bas, aucune ambassade, de quelque pays que ce soit, n'est soumise à la législation néerlandaise sur la protection des données, puisque toutes les ambassades sont dotées d'un statut particulier en vertu du droit international. Une violation de la sécurité des données dans le cadre des activités d'une ambassade n'entraînerait donc pas l'application de la législation néerlandaise sur la protection des données, ni des mesures d'exécution normalement prévues en pareil cas.

Une organisation non gouvernementale ayant des bureaux dans les États membres de l'UE ne bénéficie pas, en principe, d'une telle exonération, à moins qu'un accord international conclu avec le pays hôte ne le prévoie explicitement.

III.3. Le responsable du traitement n'est pas établi sur le territoire de l'UE mais traite des données en utilisant des moyens situés sur le territoire d'un État membre [article 4, paragraphe 1, point c)]

L'article 4, paragraphe 1, point c), vise à garantir le respect du droit à la protection des données à caractère personnel prévu par la directive lorsque le responsable du traitement n'est pas établi sur le territoire de l'Union ou de l'EEE, mais que le traitement de données à caractère personnel présente un lien évident avec ledit territoire, comme indiqué au considérant 20[22].

L'article 4, paragraphe 1, point c), prévoit l'application du droit national d'un État membre lorsque «*le responsable du traitement n'est pas établi sur le territoire de la Communauté et recourt, à des fins de traitement de données à caractère personnel, à des moyens, automatisés ou non, situés sur le territoire dudit État membre, sauf si ces moyens ne sont utilisés qu'à des fins de transit sur le territoire de la Communauté*».

Cette disposition présente un intérêt tout particulier au regard du développement des nouvelles technologies, notamment de l'internet, qui facilitent la collecte et le traitement de données à caractère personnel à distance, et ce, que le responsable du traitement soit physiquement présent ou non sur le territoire de l'Union ou de l'EEE[23].

> a) «[…] le responsable du traitement n'est pas établi sur le territoire de la Communauté […]»

Cette disposition présente un intérêt lorsque le responsable du traitement ne dispose pas, sur le territoire de l'Union ou de l'EEE, d'installation pouvant être qualifiée d'établissement au sens de l'article 4, paragraphe 1, point a), de la directive (voir analyse ci-dessus).

---

22 Considérant 20: «considérant que l'établissement, dans un pays tiers, du responsable du traitement de données ne doit pas faire obstacle à la protection des personnes prévue par la présente directive; que, dans ce cas, il convient de soumettre les traitements de données effectués à la loi de l'État membre dans lequel des moyens utilisés pour le traitement de données en cause sont localisés et de prendre des garanties pour que les droits et obligations prévus par la présente directive soient effectivement respectés».

23 Voir le document de travail intitulé «Application internationale du droit de l'UE en matière de protection des données au traitement des données à caractère personnel sur Internet par des sites web établis en dehors de l'UE» (WP 56).

Il importe de préciser l'interprétation des termes «n'est pas établi». Il est en effet essentiel de bien comprendre que l'article 4, paragraphe 1, point c), ne s'applique que lorsque l'article 4, paragraphe 1, point a), n'est pas applicable, c'est-à-dire lorsque le responsable du traitement ne dispose d'aucun établissement *pertinent au regard des activités en question* dans l'Union ou l'EEE. Ainsi, le fait qu'un responsable du traitement établi en dehors de l'Union ou de l'EEE recourt à des moyens situés dans un État membre A, dans lequel il ne dispose d'aucun établissement, n'entraînera pas l'applicabilité du droit de cet État membre si le responsable du traitement possède déjà un établissement dans un État membre B et s'il traite les données à caractère personnel dans le cadre des activités de cet établissement. Dans ce cas, tant les traitements effectués dans l'État membre A (dans lequel se trouvent les moyens utilisés) que ceux ayant lieu dans l'État membre B (où l'établissement est situé) sont soumis à la législation de ce dernier. Le groupe de travail l'a expliqué dans son avis sur les aspects de la protection des données liés aux moteurs de recherche[24].

En revanche, l'article 4, paragraphe 1, point c), s'applique lorsque le responsable du traitement possède un établissement «non pertinent» dans l'UE, c'est-à-dire lorsqu'il dispose d'établissements dans l'UE mais que leurs activités sont *sans rapport avec le traitement de données à caractère personnel.* Ces établissements n'entraînent pas l'application de l'article 4, paragraphe 1, point a).

Il s'ensuit que, puisqu'il ne doit pas y avoir de lacune ni d'incohérence dans l'application des dispositions de la directive, l'application du critère des «moyens» n'a pas à être empêchée par un établissement «non pertinent»: elle ne peut être empêchée par l'existence d'un établissement que dans la mesure où ce dernier a traité des données à caractère personnel dans le cadre des mêmes activités.

Il découle de cette interprétation qu'une entreprise exerçant diverses activités est susceptible d'entraîner l'application des points a) et c) de l'article 4, paragraphe 1, si elle recourt à des moyens et à ses établissements dans différents contextes. En d'autres termes, un responsable du traitement qui est établi en dehors de l'Union ou de l'EEE et qui recourt à des moyens situés dans l'UE doit respecter l'article 4, paragraphe 1, point c), même s'il possède un établissement dans l'UE, tant que cet établissement traite des données à caractère personnel *dans le cadre d'autres activités*. Cet établissement entraînera l'application de l'article 4, paragraphe 1, point a), pour ces activités spécifiques.

La révision du cadre juridique de l'UE régissant la protection des données offrira peut-être l'occasion de clarifier le champ d'application de l'article 4, paragraphe 1, point c), et l'expression «le responsable du traitement n'est pas établi sur le territoire de la Communauté», conformément à l'esprit de la directive et au libellé de son considérant 20. Le préambule de la directive indique clairement que l'objectif consiste à protéger les personnes et à éviter les lacunes dans l'application des principes. C'est pourquoi le groupe de travail considère que l'article 4, paragraphe 1, point c), doit s'appliquer dans les cas où il n'y a pas, dans l'Union ou l'EEE, d'établissement *susceptible d'entraîner l'application de l'article 4, paragraphe 1, point a),* ou lorsque le traitement n'est *pas effectué dans le cadre* des activités d'un tel établissement.

[24] Avis 1/2008 sur les aspects de la protection des données liés aux moteurs de recherche (WP 148).

b) «[…] et recourt, à des fins de traitement de données à caractère personnel, à des moyens, automatisés ou non, situés sur le territoire dudit État membre […]»

C'est le recours à des moyens situés sur le territoire d'un État membre qui détermine l'applicabilité de cette disposition, et donc de la législation de cet État membre en matière de protection des données.

Le groupe de travail a déjà expliqué que la notion de «recours» présuppose deux éléments: un certain type d'activité entreprise par le responsable et son intention non équivoque de traiter des données à caractère personnel[25]. Par conséquent, bien que l'utilisation de moyens situés sur le territoire de l'Union ou de l'EEE n'entraîne pas systématiquement l'application de la directive, il n'est pas nécessaire que le responsable du traitement exerce un contrôle total sur ces moyens, ni qu'il en soit propriétaire, pour que le traitement relève du champ d'application de la directive.

Il convient de remarquer qu'il y a une différence entre le terme mentionné dans la version anglaise de l'article 4, paragraphe 1, point c), à savoir «equipment», et le terme employé dans les autres versions linguistiques de la disposition («moyens» dans le texte en français), qui est plus proche du terme anglais «means». La terminologie retenue dans ces autres versions linguistiques concorde du reste avec la formulation de l'article 2, point d), qui définit le responsable du traitement comme la personne qui détermine les finalités et les moyens («means» en anglais) du traitement.

Dès lors, le groupe de travail interprète le terme «equipment» comme signifiant «means» (moyens)[26]. Il relève de surcroît que, selon la directive, ces moyens peuvent être «automatisés ou non».

Il en découle une interprétation large de ce critère, qui englobe ainsi les intermédiaires humains ou techniques, comme dans le cas des enquêtes ou des sondages. Le critère s'applique donc à la collecte d'informations au moyen de questionnaires, comme, par exemple, dans le cadre de certains essais pharmaceutiques.

Se pose alors la question de savoir si les activités externalisées, auprès de sous-traitants notamment, qui sont exercées sur le territoire de l'Union ou de l'EEE pour le compte de responsables du traitement établis en dehors de l'EEE peuvent être considérées comme des «moyens». L'interprétation large préconisée ci-dessus appelle une réponse positive, pour autant que ces activités n'entrent pas dans le cadre de celles d'un établissement du responsable du traitement situé dans l'EEE, auquel cas l'article 4, paragraphe 1, point a), s'appliquerait. Il convient toutefois de prendre en considération les conséquences parfois indésirables d'une telle interprétation, décrites au point III.4 ci-dessous: un responsable du traitement établi dans différents pays du monde qui ferait traiter des données dans un État membre de l'UE, dans lequel la base de données et le sous-traitant seraient situés, devrait se conformer à la législation de cet État membre en matière de protection des données.

---

25 WP 56, op. cit.

26 Il convient en outre de rappeler que les précédentes versions anglaises de la directive (par exemple, la proposition modifiée de 1992 – COM (92) 422 final) mentionnaient également le terme «means», qui fut modifié au cours des négociations, assez tardivement, pour retenir «equipment», comme on peut le voir dans la position commune de mars 1995.

La façon dont les moyens sont effectivement utilisés pour collecter et traiter des données à caractère personnel doit faire l'objet d'une évaluation au cas par cas. En s'appuyant sur ce raisonnement, le groupe de travail a admis la possibilité que les collectes de données à caractère personnel effectuées via les ordinateurs des utilisateurs, comme par exemple dans le cas des cookies ou des bannières en JavaScript, entraînent l'application de l'article 4, paragraphe 1, point c), et donc du droit de l'UE en matière de protection des données, aux prestataires de services établis dans des pays tiers[27].

Cette interprétation de la notion de «recours à des moyens» privilégie un large champ d'application. Toutefois, comme il a été indiqué précédemment, elle entraîne également des conséquences non satisfaisantes, lorsqu'elle aboutit à l'application de la législation européenne sur la protection des données dans des situations où le lien avec l'UE est limité (par exemple, dans le cas d'un responsable du traitement établi en dehors de l'UE qui traiterait les données concernant des non-résidents de l'Union en ayant exclusivement recours à des moyens situés dans l'UE). Il est manifestement nécessaire de parvenir à une plus grande clarté et de compléter les conditions d'application de ce critère, afin d'accroître la sécurité juridique du futur cadre qui régira la protection des données. Ce point est développé dans les conclusions du présent document.

Pour illustrer ce manque de clarté, on peut également mentionner qu'il n'est pas évident de déterminer dans quelle mesure il faut considérer les terminaux de télécommunication ou certaines parties de ceux-ci comme des moyens. Le fait que l'outil soit conçu ou essentiellement utilisé pour collecter ou traiter ultérieurement des données à caractère personnel peut servir d'indicateur à cet égard. Il n'en demeure pas moins que lorsqu'un responsable du traitement collecte sciemment des données à caractère personnel, même accessoirement, en ayant recours à des moyens situés dans l'UE, la directive s'applique.

Exemple n° 7: services de géolocalisation

Une entreprise implantée en Nouvelle-Zélande utilise des véhicules dans le monde entier, notamment dans les États membres de l'UE, pour recueillir des informations sur les points d'accès Wi-Fi (dont des informations concernant les appareils terminaux dont disposent les particuliers) afin de fournir un service de géolocalisation à ses clients. Cette activité implique souvent le traitement de données à caractère personnel.

La directive sur la protection des données est applicable pour deux raisons:
- premièrement, les véhicules qui collectent des informations sur les points d'accès Wi-Fi en circulant dans la rue peuvent être considérés comme des moyens au sens de l'article 4, paragraphe 1, point c);
- deuxièmement, pour fournir le service de géolocalisation, le responsable du traitement utilise le dispositif mobile de la personne concernée (grâce à un logiciel spécialisé installé dans le dispositif) comme moyen pour fournir des informations sur la localisation du dispositif et de son utilisateur.

Tant la collecte des informations nécessaires pour fournir le service que la fourniture du service de géolocalisation proprement dit doivent respecter les dispositions de la directive.

[27] WP 56, op. cit., pages 11 et suivantes.

Exemple nº 8: informatique dématérialisée

L'informatique dématérialisée, qui permet de traiter des données à caractère personnel et de les enregistrer sur des serveurs répartis dans le monde, est un exemple complexe d'application des dispositions de la directive. L'endroit exact où les données se trouvent n'est pas toujours connu et il peut changer au fil du temps, mais cela n'est pas déterminant pour définir le droit applicable. Il suffit que le responsable du traitement effectue celui-ci dans le cadre des activités d'un établissement sur le territoire de l'Union, ou qu'il utilise des moyens situés sur ce territoire, pour que le droit européen soit applicable, conformément à l'article 4, paragraphe 1, point c), de la directive.

La première chose à faire est de déterminer qui est le responsable du traitement et quelles activités ont lieu dans quel cadre. On peut distinguer deux cas de figure:

l'utilisateur du service «en nuage» («cloud service») est responsable du traitement: par exemple, une entreprise recourt à un service d'agenda en ligne pour organiser ses rendez-vous avec ses clients. Si l'entreprise utilise le service dans le cadre des activités de son établissement situé dans l'UE, le droit de l'UE s'applique aux traitements de données effectués via l'agenda en ligne, conformément à l'article 4, paragraphe 1, point a), de la directive. L'entreprise doit s'assurer que le service offre des garanties appropriées pour assurer la protection des données, notamment en ce qui concerne la sécurité des données à caractère personnel stockées dans le «nuage». Elle doit également informer ses clients des finalités pour lesquelles les données les concernant sont utilisées, ainsi que des conditions d'utilisation de ces données;

dans certains cas, le fournisseur du service «en nuage» peut également être responsable du traitement, par exemple lorsqu'il met à disposition un agenda en ligne, où les particuliers peuvent inscrire tous leurs rendez-vous personnels, et qu'il propose des services à valeur ajoutée, tels que la synchronisation des rendez-vous et des contacts. Si le fournisseur du service «en nuage» a recours à des moyens situés dans l'UE, il est soumis à la législation européenne sur la protection des données en vertu de l'article 4, paragraphe 1, point c). Ainsi qu'il est expliqué ci-dessous, la directive ne s'appliquera pas si les moyens ne sont utilisés qu'à des fins de transit. En revanche, l'utilisation de moyens plus spécifiques entraînera son application, par exemple si le service utilise des fonctionnalités de calcul, exécute des scripts en Java ou installe des cookies dans le but d'enregistrer et de récupérer les données à caractère personnel des utilisateurs. Dans ce cas, le fournisseur du service «en nuage» doit informer les utilisateurs des modalités selon lesquelles les données sont traitées, enregistrées et, éventuellement, accessibles à des tiers, ainsi que garantir des mesures de sécurité appropriées pour protéger ces données.

Exemple nº 9: un responsable du traitement publie des listes nationales de pédophiles

Un responsable du traitement établi dans un État membre de l'UE ou de l'EEE publie des listes nationales de personnes soupçonnées d'avoir commis des infractions pénales à l'encontre de mineurs ou condamnées pour de tels actes. Pour ce qui concerne la protection des données à caractère personnel relatives aux personnes figurant sur ces listes, le droit applicable, au regard duquel la licéité du traitement de ces données doit être évaluée, est celui de l'État membre dans lequel le responsable du traitement est établi.

Le fait que le responsable du traitement ait ou non recours à des moyens situés dans d'autres États membres [comme des serveurs internet ayant des noms de domaine de premier niveau différents (.fr, .it, .pl, etc.)], ou qu'il cible ou non directement les citoyens d'autres États membres de l'UE (par exemple, en publiant pour chacun de ces pays une liste de noms dans la langue du pays en question), importe peu pour la détermination du droit applicable en matière de protection des données.

Quoi qu'il en soit, l'autorité de contrôle de l'État membre d'établissement peut être invitée par d'autres autorités de contrôle à coopérer, en statuant sur des plaintes déposées par des personnes résidant dans d'autres États membres.

Bien entendu, des critères de rattachement différents, et donc des législations différentes peuvent s'appliquer dans d'autres domaines du droit, par exemple, pour engager des poursuites pour diffamation en matière civile ou pénale.

c) «[…] sauf si ces moyens ne sont utilisés qu'à des fins de transit sur le territoire de la Communauté […]»

L'application du droit national d'un État membre de l'UE dans lequel sont situés des moyens auxquels le responsable du traitement a recours est exclue lorsque ces moyens ne servent qu'à assurer un transit sur le territoire de l'Union, comme, par exemple, dans le cas des réseaux de télécommunication (câbles) ou des services postaux qui assurent seulement le transit par l'Union des communications destinées à des pays tiers.

S'agissant d'une exception au critère des moyens, une interprétation étroite s'impose. Il convient de noter que l'application effective de cette exception devient rare: dans la pratique, les services de télécommunication sont de plus en plus nombreux à fusionner les services de transit et les services à valeur ajoutée, comme le filtrage anti-spam ou autres services de manipulation des données à l'occasion de leur transmission. La simple transmission par câble de point à point disparaît peu à peu. Il conviendra d'en tenir compte lors de la révision du cadre juridique de la protection des données.

d) «[…] doit désigner un représentant établi sur le territoire dudit État membre […]» (article 4, paragraphe 2)

La directive fait obligation au responsable du traitement de désigner «un représentant» sur le territoire de l'État membre dont le droit est applicable en raison du recours par le responsable du traitement à des moyens situés dans cet État membre, à des fins de traitement de données à caractère personnel. Cela s'entend «sans préjudice d'actions qui pourraient être introduites contre le responsable du traitement lui-même».

Dans ce dernier cas, la question de l'opposabilité à un représentant pose des problèmes pratiques, comme le montre l'expérience des États membres. Il en serait ainsi, par exemple, si l'unique représentant du responsable du traitement sur le territoire de l'Union était un cabinet d'avocats. Les dispositions nationales transposant la directive n'apportent pas de réponse uniforme à la question de savoir si le représentant peut être tenu pour responsable et sanctionné, en matière civile ou pénale, au nom du responsable du traitement. La nature de la relation entre ce dernier et son représentant est déterminante à cet égard. Dans certains États membres, le représentant se substitue au responsable du traitement, y compris sur le plan répressif, tandis que dans d'autres, il n'a qu'un simple mandat. Alors que certaines lois nationales prévoient expressément des amendes à l'encontre des représentants[28], cette possibilité n'est pas envisagée dans d'autres États membres[29].

Une harmonisation sur ce point s'impose au niveau européen, afin de donner un rôle plus effectif aux représentants. En particulier, les personnes concernées devraient pouvoir exercer leurs droits à son encontre, sans préjudice d'actions qui pourraient être introduites contre le responsable du traitement lui-même.

III.4. Considérations relatives aux conséquences concrètes de l'application de l'article 4, paragraphe 1, point c)

Un aspect fondamental de l'application de l'article 4, paragraphe 1, point c), concerne ses conséquences concrètes pour le responsable du traitement. Bien qu'établi en dehors de l'Union ou de l'EEE, le responsable du traitement doit se conformer aux principes de la directive s'il recourt, à des fins de traitement de données à caractère personnel, à des moyens situés sur le territoire de l'Union. On peut se demander si les principes de la directive ne s'appliquent alors qu'aux traitements effectués dans l'UE ou au responsable du traitement en tant que tel, pour toutes les étapes des traitements, y compris celles qui se déroulent dans un pays tiers. Ces questions revêtent une importance particulière dans le cas des environnements en réseau, tels que l'informatique dématérialisée, ou des entreprises multinationales.

Prenons l'exemple de responsables du traitement établis dans divers pays du monde, qui font traiter leurs données en France, où la base de données et les moyens de traitement sont situés. Si les différents responsables du traitement ont recours à des infrastructures situées en France, l'article 4, paragraphe 1, point c), est applicable, et tous les responsables doivent se conformer au droit français. Cela peut avoir des conséquences indésirables sur le plan économique et de l'opposabilité.

Des considérations pratiques plaideraient en faveur d'une limitation de l'application des critères liés aux moyens, mais elles sont contrebalancées par le fait que les principes de protection des données visent à protéger un droit fondamental. Il ne paraît pas admissible de restreindre les droits des personnes à certaines parties du traitement des données les

[28] Voir la loi belge du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel (Moniteur belge du 18 mars 1993), ainsi que la loi néerlandaise du 6 juillet 2000 relative à la protection des données à caractère personnel (*Staatsblad* n° 302 du 20 juillet 2000). Voir également la législation grecque [article 3, paragraphe 3, point b), en liaison avec l'article 21, paragraphe 1, de la loi n° 2472/1997).

[29] La loi française n° 78/17 du 6 janvier 1978, par exemple, ne prévoit pas ce type d'amendes à l'encontre des représentants.

concernant. Il ne serait pas non plus acceptable de réduire l'étendue de la protection aux personnes résidant dans l'UE, le droit fondamental à la protection des données à caractère personnel étant reconnu indépendamment de la nationalité ou du lieu de résidence. Par conséquent, il résulte du critère de l'article 4, paragraphe 1, point c), que les principes de la directive s'appliquent au responsable du traitement proprement dit, pour toutes les étapes des traitements, y compris celles qui se déroulent dans un pays tiers.

Il convient donc de considérer que la directive s'applique à un responsable du traitement pour toutes les étapes d'un traitement tant que le lien avec l'UE est effectif et non ténu (comme ce serait le cas, par exemple, si l'utilisation de moyens situés dans un État membre était pratiquement involontaire).

Comme il est expliqué dans les conclusions, un facteur de rattachement plus précis qui, pour compléter les critères liés aux moyens, tiendrait compte du degré de «ciblage» des personnes, pourrait être utile sur le plan de la sécurité juridique. Le critère du ciblage n'est pas nouveau. Il a déjà été utilisé dans d'autres contextes dans l'UE[30], ainsi qu'aux États-Unis dans la législation sur la protection des enfants sur internet[31]. Il est également retenu par certaines lois nationales transposant la directive 2000/31/CE sur le commerce électronique[32], qui prévoient que les prestataires non établis dans l'EEE relèvent de leur champ d'application si les services qu'ils proposent visent spécifiquement le territoire national.

L'application d'un critère similaire pour la législation de l'UE en matière de protection des données pourrait faire l'objet d'une réflexion lors des futures discussions sur la révision du cadre juridique dans ce domaine.

Une autre conséquence pratique de l'application de l'article 4, paragraphe 1, point c), concerne l'interaction entre cette disposition et les articles 25 et 26 de la directive. Le fait qu'un responsable du traitement établi en dehors de l'Union ou de l'EEE recoure à des moyens situés sur le territoire de l'Union ou de l'EEE, et qu'il doive donc respecter toutes les dispositions pertinentes de la directive, pourrait également entraîner l'applicabilité des articles 25 et 26. Toutefois, dans la pratique, il serait difficile de déterminer précisément les conséquences d'un tel scénario.

Par exemple, si un responsable du traitement X établi en dehors de l'EEE collecte des données à caractère personnel en ayant recours à des moyens situés sur le territoire de l'Union (par exemple à l'aide de cookies ou par l'intermédiaire d'un sous-traitant), il doit se conformer à la directive pour toutes les étapes du traitement. On peut établir ici un parallèle avec la situation où un responsable du traitement établi dans l'EEE transfère des

---

30 Voir l'article 15, paragraphe 1, point c), du règlement (CE) n° 44/2001 du Conseil du 22 décembre 2000 concernant la compétence judiciaire, la reconnaissance et l'exécution des décisions en matière civile et commerciale (JO L 12 du 16.1.2001, p. 1) et, pour son interprétation, les conclusions de l'avocat général Trstenjak du 18 mai 2010 dans l'affaire C-144/09, *Hotel Alpenhof*.

31 En effet, la loi COPPA (*Children's Online Privacy Protection Act*) s'applique si un éditeur est établi aux États-Unis ou si un site web cible les enfants américains: les sites web et les services en ligne étrangers doivent respecter cette loi s'ils s'adressent à des enfants aux États-Unis ou s'ils collectent sciemment des données à caractère personnel auprès d'enfants aux États-Unis. Cf. 16 CFR 312.2, disponible à l'adresse http://www.ftc.gov/os/1999/10/64fr59888.pdf, p. 59912.

32 Directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur («directive sur le commerce électronique»), JO L 178 du 17.7.2000, p. 1.

données à caractère personnel vers un sous-traitant situé en dehors de l'EEE: dans ce cas, le responsable du traitement et le sous-traitant établi en dehors du territoire de l'EEE sont également soumis aux dispositions de la directive. Cependant, les modalités d'application pratique de ces principes, conformément aux exigences des articles 25 et 26 de la directive quant au caractère adéquat du niveau de protection, dans le cas de figure exposé à l'article 4, paragraphe 1, point c), où le responsable du traitement est établi en dehors de l'EEE, ne sont pas parfaitement claires. Le groupe de travail estime qu'il conviendrait de procéder à un examen approfondi des instruments qui régissent les conditions applicables aux transferts afin de mieux couvrir ce cas de figure.

III.5. Droit applicable aux mesures de sécurité (article 17, paragraphe 3)

L'article 17, paragraphe 3, prévoit que le contrat ou l'acte juridique qui lie le sous-traitant au responsable du traitement doit également garantir le respect des mesures de sécurité «définies par la législation de l'État membre dans lequel le sous-traitant est établi».

Ce principe s'explique par la nécessité de garantir des exigences uniformes au sein d'un même État membre en matière de mesures de sécurité et d'en faciliter l'application. Il convient toutefois de relever que les exigences en matière de sécurité divergent sensiblement selon les États membres de l'UE: alors que certains prévoient des règles très détaillées, d'autres se sont contentés de reproduire le libellé général de la directive. Les lois nationales qui sont générales et dont le texte est identique à celui de la directive sont sans conséquence pratique. Il ne poserait aucun problème à un sous-traitant de respecter des obligations plus détaillées imposées par le responsable du traitement en vertu de sa législation nationale, ou à un responsable du traitement d'accepter des exigences plus détaillées au titre de la législation dont relève le sous-traitant. Ce n'est que dans le cas où les règles détaillées sont différentes, voire contradictoires, que l'article 17, paragraphe 3, tranche en faveur de la législation du pays dans lequel le sous-traitant est établi[33]. Il conviendrait néanmoins de songer à une plus grande harmonisation des obligations en matière de sécurité lors de la révision du cadre juridique de la protection des données.

III.6. Compétences des autorités de contrôle et coopération entre celles-ci (article 28, paragraphe 6)

Comme il a été mentionné précédemment (voir point II.2.d)), l'article 28, paragraphe 6, vise à combler l'écart susceptible d'apparaître, sur le marché intérieur, entre le droit applicable et les compétences de contrôle dans le domaine de la protection des données.

Conformément à cette disposition, les autorités nationales chargées de la protection des données ont compétence pour surveiller l'application de la législation dans ce domaine sur le territoire de l'État membre dont elles relèvent. Toutefois, si le droit d'un autre État membre est applicable sur le territoire de l'État dont elle relève, les pouvoirs d'exécution de l'autorité chargée de la protection des données n'en sont pas pour autant limités: les critères fixés par la directive concernant le droit applicable prévoient la possibilité qu'une autorité chargée de la protection des données soit habilitée à vérifier un traitement

[33] Cela doit permettre d'éviter que la désignation d'un sous-traitant dans un pays imposant des obligations moins strictes puisse être considérée comme une violation des obligations du responsable du traitement.

effectué sur le territoire de l'État dont elle relève et à intervenir à ce sujet, même si le droit applicable est celui d'un autre État membre.

III.6.a) «Indépendamment du droit national applicable […], chaque autorité de contrôle a compétence […]»

Cette disposition autorise une autorité nationale de contrôle à intervenir, dans les limites de sa compétence territoriale, dans tous les cas de figure, que le droit applicable en matière de protection des données soit celui de l'État dont elle relève ou celui d'un autre État membre.

III.6.b) «[…] pour exercer, sur le territoire de l'État membre dont elle relève, les pouvoirs dont elle est investie […]»

De même, lorsque c'est le droit d'un autre État membre qui est applicable en matière de protection des données, l'autorité de contrôle peut exercer, sur son territoire, tous les pouvoirs qui lui sont conférés par l'ordre juridique national (pouvoirs d'investigation, pouvoirs d'intervention, pouvoir d'ester en justice, pouvoir d'infliger des sanctions, etc.).

Lorsque plusieurs autorités chargées de la protection des données sont concernées, notamment celle du lieu où le traitement est effectué et celles dont le droit est applicable, il est essentiel que leur coopération soit organisée et que le rôle de chacune d'elles soit clairement défini. Il convient dès lors de se pencher sur plusieurs questions, à savoir notamment:

- les questions de procédure, telles que la détermination de l'autorité chef de file et la manière dont elle coopérera avec les autres autorités;
- l'étendue des compétences de chaque autorité. Il s'agit en particulier de déterminer la mesure dans laquelle l'autorité du lieu où le traitement est effectué exercera ses pouvoirs, s'agissant de l'application des principes matériels et des sanctions; de savoir si elle doit limiter l'exercice de ses pouvoirs à la vérification des faits et si elle peut prendre des mesures d'exécution provisoires, voire même des mesures définitives; de savoir si elle peut donner sa propre interprétation des dispositions du droit applicable ou s'il s'agit là d'une prérogative de l'autorité de l'État membre dont le droit est applicable. Il convient de relever à cet égard que toutes les lois nationales ne prévoient pas la possibilité d'infliger des sanctions à tous les intervenants.[34]

Un degré élevé d'harmonisation des pouvoirs de surveillance dont les autorités de contrôle sont investies conformément à l'article 28 de la directive est une condition essentielle pour garantir, de manière effective et non discriminatoire, le respect des dispositions relatives à la protection des données au-delà des frontières. Considérant que cette question nécessite une analyse approfondie, le groupe de travail fournira des indications à ce sujet dans un document distinct.

Exemple nº 10: traitements transfrontières dans l'UE de données à caractère personnel

Des traitements sont effectués au Royaume-Uni, mais dans le cadre des activités d'un établissement du responsable du traitement situé en Allemagne. Il s'ensuit que:

- le droit allemand s'applique aux traitements effectués au Royaume-Uni;

[34] La loi grecque, par exemple, ne prévoit des sanctions qu'à l'encontre des responsables du traitement et de leurs représentants. Elle n'en prévoit pas à l'encontre des sous-traitants.

- l'autorité britannique chargée de la protection des données doit avoir le pouvoir d'inspecter les locaux au Royaume-Uni et d'établir des conclusions, à transmettre à son homologue allemande;

- cette dernière doit pouvoir infliger une sanction au responsable du traitement établi en Allemagne, sur la base des conclusions de l'autorité britannique.

De plus, si l'établissement au Royaume-Uni est un sous-traitant, les aspects liés à la sécurité des traitements sont soumis aux exigences du droit britannique en matière de protection des données. Se pose alors la question de savoir comment veiller à la bonne application de ces exigences.

III.6.c) «[…] coopèrent entre elles dans la mesure nécessaire à l'accomplissement de leurs missions […]»

Les autorités de contrôle sont tenues de coopérer, mais cette obligation se limite à ce qui est nécessaire pour accomplir leurs missions. Les demandes de coopération doivent donc être en rapport avec l'exercice de leurs compétences. Elles portent en général sur des affaires transfrontières.

Cette disposition évoque en particulier l'échange de «toute information utile» concernant, par exemple, les dispositions pertinentes et les instruments juridiques applicables à la situation en cause. Toutefois, la coopération peut se concrétiser à différents niveaux: traitement de plaintes transfrontières, recherche de preuves pour d'autres autorités chargées de la protection des données, ou application de sanctions.

La question est encore plus délicate dans le contexte international, c'est-à-dire lorsque des responsables du traitement exercent leurs activités au niveau mondial. Elle nécessite des améliorations de la coopération en matière répressive. Des initiatives telles que le *Global Privacy Enforcement Network* (GPEN), réseau d'autorités chargées de la protection des données de différents continents, représentent une avancée nécessaire et utile dans ce sens.

Exemple n° 11: réseau social ayant son siège dans un pays tiers et un établissement dans l'UE

Une plateforme de réseau social a son siège dans un pays tiers et un établissement dans un État membre. L'établissement définit et applique les politiques relatives au traitement des données à caractère personnel concernant les résidents de l'UE. Le réseau social cible activement les résidents de tous les États membres de l'UE, qui représentent une part importante de ses clients et de ses recettes. Il installe également des cookies sur les ordinateurs des utilisateurs dans l'UE.

Dans ce cas, conformément à l'article 4, paragraphe 1, point a), le droit applicable en matière de protection des données est celui de l'État membre de l'UE sur le territoire duquel l'entreprise est établie. Peu importe que le réseau social recoure ou non à des moyens situés sur le territoire d'autres États membres, puisque tous les traitements sont effectués dans le cadre des activités de l'établissement unique et que la directive exclut l'application cumulée des points a) et c) de l'article 4, paragraphe 1.

Toutefois, en application de l'article 28, paragraphe 6, l'autorité de contrôle de l'État membre sur le territoire duquel le réseau social est établi est tenue de coopérer avec les autres autorités de contrôle, par exemple pour traiter les demandes ou les réclamations émanant de résidents d'autres États membres de l'UE.

Exemple nº 12: plateforme européenne en matière de santé en ligne

Une plateforme est créée au niveau européen afin de faciliter le traitement transfrontière des dossiers médicaux. La plateforme permet l'échange d'informations sur les patients (informations générales, antécédents médicaux et traitements en cours), afin de faciliter les prestations de soins à l'occasion de séjours à l'étranger.

Bien que la plateforme facilite l'échange d'informations, il n'en existe pas moins, dans chaque État membre, un ou plusieurs établissements dans le cadre des activités desquels les informations relatives aux patients sont traitées. Par exemple, si un résident bulgare voyageant au Portugal nécessite un traitement médical urgent, son dossier sera traité, via la plateforme, par les services médicaux portugais conformément au droit portugais en matière de protection des données. Si, après son retour en Bulgarie, le patient souhaite déposer une réclamation au sujet du traitement des données le concernant effectué par le responsable du traitement portugais, il doit s'adresser en premier lieu à l'autorité chargée de la protection des données en Bulgarie. Cette dernière collaborera avec son homologue portugaise pour établir les faits et déterminer s'il y a lieu violation de la législation portugaise.

Si la Commission européenne intervient dans le fonctionnement de la plateforme en organisant les flux de données à caractère personnel et en garantissant la sécurité du système, cela peut également être considéré comme un traitement de données à caractère personnel, auquel cas le règlement (CE) n° 45/2001 est d'application. Dans ce cas de figure, si le citoyen bulgare dépose une réclamation pour violation de la sécurité de ses données médicales, l'autorité chargée de la protection des données en Bulgarie collaborera avec le Contrôleur européen de la protection des données (CEPD) afin d'établir les circonstances et les conséquences de cette violation.

IV. Conclusions

Le présent avis vise avant tout à clarifier le champ d'application de la directive 95/46/CE, et en particulier de son article 4, mais également à dégager les domaines dans lesquels des améliorations sont encore possibles. Les principales conclusions sur ces deux points sont récapitulées ci-dessous.

IV.1. Clarifier les dispositions en vigueur

Délimiter l'application du droit de l'UE aux traitements de données à caractère personnel permettra de clarifier le champ d'application de la législation européenne sur la protection des données, tant dans l'Union ou l'EEE que dans un contexte international plus large. Une bonne compréhension du droit applicable contribuera à garantir simultanément la sécurité juridique pour les responsables du traitement et un cadre clair pour les personnes concernées et les autres parties prenantes. Par ailleurs, une

compréhension correcte des dispositions relatives au droit applicable devrait permettre de prévenir toute lacune dans le niveau élevé de protection des données à caractère personnel prévu par la directive 95/46.

La principale disposition concernant le droit applicable est l'article 4, qui détermine quelle(s) loi(s) nationale(s) en matière de protection de données, adoptée(s) conformément à la directive, peu(ven)t s'appliquer aux traitements de données à caractère personnel.

En vertu de l'article 4, paragraphe 1, point a), un État membre doit appliquer sa législation nationale sur la protection des données lorsque le traitement est effectué dans le cadre des activités d'un établissement du responsable du traitement situé sur son territoire. Pour définir si un établissement relève de ladite disposition, il est déterminant de savoir s'il exerce effectivement et réellement les activités. En outre, la référence à «un» établissement signifie que la présence d'un établissement du responsable du traitement sur le territoire d'un État membre entraîne l'applicabilité du droit de cet État, et que la présence d'autres établissements de ce même responsable sur le territoire d'autres États membres peut entraîner l'applicabilité du droit de ces États.

La notion de «cadre des activités», et non la localisation des données, est un facteur déterminant pour la définition du droit applicable. Cette notion suppose que le droit applicable n'est pas celui de l'État membre dans lequel le *responsable du traitement* est établi, mais celui de l'État dans lequel un *établissement* du responsable du traitement participe à des *activités* impliquant le traitement de données à caractère personnel. Dans ce contexte, le degré de participation du ou des établissements aux activités dans le cadre desquelles des données à caractère personnel sont traitées revêt une importance capitale. De plus, il convient de prendre en considération la nature des activités des établissements, ainsi que la nécessité d'assurer la protection effective des droits des personnes. Il y a lieu d'adopter une approche fonctionnelle pour analyser ces critères: ce sont davantage le comportement des parties et leur interaction que leur évaluation théorique du droit applicable qui sont déterminants.

L'article 4, paragraphe 1, point b), règle la situation, moins courante, où la législation d'un État membre en matière de protection des données s'applique lorsque «le responsable du traitement n'est pas établi sur le territoire de l'État membre mais en un lieu où sa loi nationale s'applique en vertu du droit international public». Certains critères extérieurs, issus du droit international public, peuvent avoir pour effet, dans des situations particulières, d'étendre l'application d'une législation nationale sur la protection des données au-delà des frontières nationales, comme dans le cas des ambassades ou des navires.

L'article 4, paragraphe 1, point c), vise à garantir le respect du droit à la protection des données à caractère personnel prévu par la directive même dans les cas où le responsable du traitement n'est pas établi sur le territoire de l'Union ou de l'EEE, mais où le traitement de données à caractère personnel présente un certain lien avec ledit territoire. Afin d'assurer la cohérence des dispositions de l'article 4 et d'éviter toute lacune dans l'application de la législation protégeant les données, le groupe de travail considère que la présence, sur le territoire de l'Union, d'un établissement du responsable du traitement qui ne relève pas de l'article 4, paragraphe 1, point a), ne devrait pas faire obstacle à l'application de l'article 4, paragraphe 1, point c). Au contraire, la partie de cette disposition concernant les «moyens utilisés» devrait s'appliquer dans les cas où il n'y a

pas, dans l'Union ou l'EEE, d'établissement *susceptible d'entraîner l'application de l'article 4, paragraphe 1, point a)*, ou lorsque le traitement n'est *pas effectué dans le cadre* des activités d'un tel établissement.

C'est le recours à des moyens situés sur le territoire d'un État membre qui détermine l'applicabilité de l'article 4, paragraphe 1, point c), et donc de la législation de cet État membre en matière de protection des données. La notion de «recours» présuppose deux éléments: un certain type d'activité entreprise par le responsable et son intention non équivoque de traiter des données à caractère personnel. Par conséquent, bien que l'utilisation de moyens situés sur le territoire de l'Union ou de l'EEE n'entraîne pas systématiquement l'application de la directive, il n'est pas nécessaire que le responsable du traitement exerce un contrôle total sur les moyens, ni qu'il en soit propriétaire, pour que le traitement relève du champ d'application de la directive.

Pour ce qui est de la notion de «moyens», les termes employés dans les différentes versions linguistiques de la directive n'étant pas parfaitement équivalents («*equipment*» et non pas «*means*» en anglais), il y a lieu de donner une interprétation large à cette notion, privilégiant ainsi un large champ d'application. Dans certains cas, une telle interprétation entraînera l'application de la législation européenne sur la protection des données à un traitement qui ne présente pas de véritable lien avec l'UE ou l'EEE. En tout état de cause, un traitement de données à caractère personnel effectué par un responsable du traitement établi hors du territoire de l'Union ou de l'EEE, en ayant recours à des moyens situés sur ce territoire, entraîne l'application de la directive, conformément à l'article 4, paragraphe 1, point c), de sorte que toutes les autres dispositions pertinentes de la directive seront également applicables.

L'application du droit national d'un État membre de l'UE dans lequel sont situés des moyens auxquels le responsable du traitement a recours est exclue lorsque ces moyens ne servent qu'à assurer un transit sur le territoire de l'Union, comme, par exemple, dans le cas des réseaux de télécommunication (câbles) ou des services postaux qui assurent seulement le transit par l'Union des communications destinées à des pays tiers.

L'article 4, paragraphe 2, fait obligation au responsable du traitement de désigner un représentant sur le territoire de l'État membre dont le droit est applicable en raison du recours par le responsable du traitement à des moyens situés dans cet État membre, à des fins de traitement de données à caractère personnel. Dans ce cas, l'opposabilité à un représentant peut poser des problèmes.

L'article 17, paragraphe 3, dispose que le contrat ou l'acte juridique qui lie le sous-traitant au responsable du traitement doit également prévoir que le sous-traitant est tenu de respecter les mesures de sécurité «*définies par la législation de l'État membre dans lequel le sous-traitant est établi*». Ce principe s'explique par la nécessité de garantir des exigences uniformes au sein d'un même État membre en matière de mesures de sécurité, et d'en faciliter l'application.

L'article 28, paragraphe 6, vise à combler l'écart susceptible d'apparaître, sur le marché intérieur, entre le droit applicable et les compétences de contrôle dans le domaine de la protection des données, en prévoyant qu'une autorité chargée de la protection des données doit être habilitée à vérifier un traitement effectué sur le territoire de l'État dont elle relève et à intervenir à ce sujet, même si le droit applicable est celui d'un autre État membre.

IV.2. Améliorer les dispositions en vigueur

Si les indications et les exemples qui viennent d'être exposés devraient permettre de renforcer la sécurité juridique et la protection des droits des personnes lors de la détermination du droit applicable au traitement de données à caractère personnel, leur développement a fait apparaître certaines faiblesses.

Ainsi, il serait utile de clarifier le libellé de la directive et d'améliorer la cohérence entre les différentes parties de l'article 4 lors de la révision du cadre général de la protection des données. Le groupe de travail estime en effet que des éclaircissements s'imposent dans plusieurs domaines:

a. il est indispensable de supprimer les incohérences entre l'article 4, paragraphe 1, point a), et l'article 4, paragraphe 1, point c), en ce qui concerne le terme «établissement», et la notion mentionnant que le responsable du traitement n'est «pas établi» sur le territoire de l'Union. Dans un souci de cohérence avec l'article 4, paragraphe 1, point a), qui retient le critère de l'«établissement», l'article 4, paragraphe 1, point c), devrait s'appliquer dans tous les cas où il n'y a pas dans l'UE d'*établissement susceptible d'entraîner l'application de l'article 4, paragraphe 1, point a)*, ou lorsque le traitement n'est *pas effectué dans le cadre* des activités d'un tel établissement;

b. il serait également judicieux de préciser la notion de «cadre des activités» de l'établissement. Le groupe de travail a souligné la nécessité d'évaluer le ***degré de participation*** du ou des établissements aux activités dans le cadre desquelles des données à caractère personnel sont traitées, c'est-à-dire de déterminer «qui fait quoi» dans quel établissement. Ce critère est interprété en tenant compte des travaux préparatoires de la directive et de l'objectif fixé à cette époque, qui consistait à conserver une approche distributive des législations nationales applicables aux différents établissements du responsable du traitement dans l'UE. Le groupe de travail considère que, dans sa version actuelle, l'article 4, paragraphe 1, point a), aboutit à une solution certes réalisable mais parfois compliquée, qui plaide en faveur d'une approche plus centralisée et harmonisée;

c. le changement envisagé pour simplifier les règles de détermination du droit applicable consisterait à revenir au principe du pays d'origine: tous les établissements d'un même responsable du traitement dans l'UE appliqueraient la même législation, indépendamment du territoire sur lequel ils seraient situés. Dans cette perspective, le premier critère à appliquer serait le lieu du principal établissement du responsable du traitement. L'existence de plusieurs établissements dans l'UE n'entraînerait pas l'application des différentes législations nationales correspondantes;

d. cette option ne serait cependant acceptable que s'il n'existe pas de différences significatives entre les législations des États membres. Dans le cas contraire, l'application effective du principe du pays d'origine encouragerait la pratique du «forum shopping» en faveur des États membres dont la législation est réputée plus laxiste à l'égard des responsables du traitement, ce qui pourrait également porter préjudice aux personnes concernées. La sécurité juridique des responsables du traitement et des personnes concernées ne pourrait être garantie que moyennant une

harmonisation générale des législations nationales, y compris des obligations en matière de sécurité. C'est pourquoi le groupe de travail est favorable à une harmonisation poussée des principes de protection des données, qu'il estime d'ailleurs indispensable pour pouvoir éventuellement passer au principe du pays d'origine;

e. des critères supplémentaires devraient s'appliquer lorsque le responsable du traitement est établi en dehors de l'UE, en vue de garantir l'existence d'un lien suffisant avec le territoire de l'Union et d'éviter que des responsables du traitement établis dans des pays tiers ne puissent utiliser ce dernier pour exercer des activités illégales de traitement de données. On peut envisager les deux critères suivants dans cette optique:

   – le ciblage des personnes ou l'«approche axée sur le service», c'est-à-dire que l'activité impliquant le traitement de données à caractère personnel doit cibler des personnes résidant dans l'UE pour entraîner l'application du droit de l'UE en matière de protection des données. Ce critère devrait reposer sur ciblage poussé, en prenant en compte le lien effectif entre la personne et un État membre de l'UE. Les exemples suivants illustrent en quoi pourrait consister le ciblage: le fait qu'un responsable du traitement collecte des données à caractère personnel dans le cadre de services explicitement accessibles ou destinés aux résidents de l'UE, par l'affichage d'informations dans les langues parlées dans l'UE; la prestation de services ou la livraison de produits dans les États membres de l'UE; le fait que l'accessibilité d'un service soit subordonnée à l'utilisation d'une carte de crédit européenne; l'envoi de publicités dans la langue du destinataire ou pour des produits et services disponibles dans l'UE. Le groupe de travail relève que ce critère est déjà utilisé dans le domaine de la protection des consommateurs. Par conséquent, l'appliquer dans le contexte de la protection des données augmenterait la sécurité juridique des responsables du traitement, puisque ceux-ci devraient appliquer le même critère pour des activités qui entraînent souvent l'application simultanée des règles de protection des consommateurs et des règles de protection des données;

   – le critère des moyens: bien que ce critère produise des conséquences indésirables, telles que l'éventuelle application universelle du droit de l'UE, il n'en demeure pas moins nécessaire d'empêcher qu'un vide juridique ne fasse de l'Union un refuge pour les données illicites («data haven»), par exemple lorsqu'une activité de traitement pose des problèmes éthiques inadmissibles. On pourrait donc conserver le critère des moyens, sous l'angle des droits fondamentaux, et sous une forme résiduelle. Il ne s'appliquerait alors qu'en troisième lieu, lorsque les deux autres critères ne pourraient être retenus: il couvrirait les cas limites (données concernant des personnes ne résidant pas dans l'UE, responsables du traitement sans lien avec l'UE) dans lesquels il existe une infrastructure pertinente dans l'UE, liée au traitement d'informations. Dans ce dernier cas, on pourrait éventuellement limiter le nombre de principes applicables, en ne conservant, par exemple, que le principe de légitimité ou de sécurité. Cette approche qui, bien entendu, nécessiterait d'être peaufinée, résoudrait probablement la plupart des problèmes posés par l'article 4, paragraphe 1, point c), dans sa version actuelle.

f. Enfin, le groupe de travail recommande une harmonisation plus poussée en ce qui concerne l'obligation faite aux responsables du traitement établis dans des pays tiers de désigner un représentant dans l'UE, afin de donner un rôle plus effectif à ce dernier. Il conviendrait en particulier de préciser dans quelle mesure les personnes concernées peuvent véritablement exercer leurs droits à l'encontre d'un représentant.

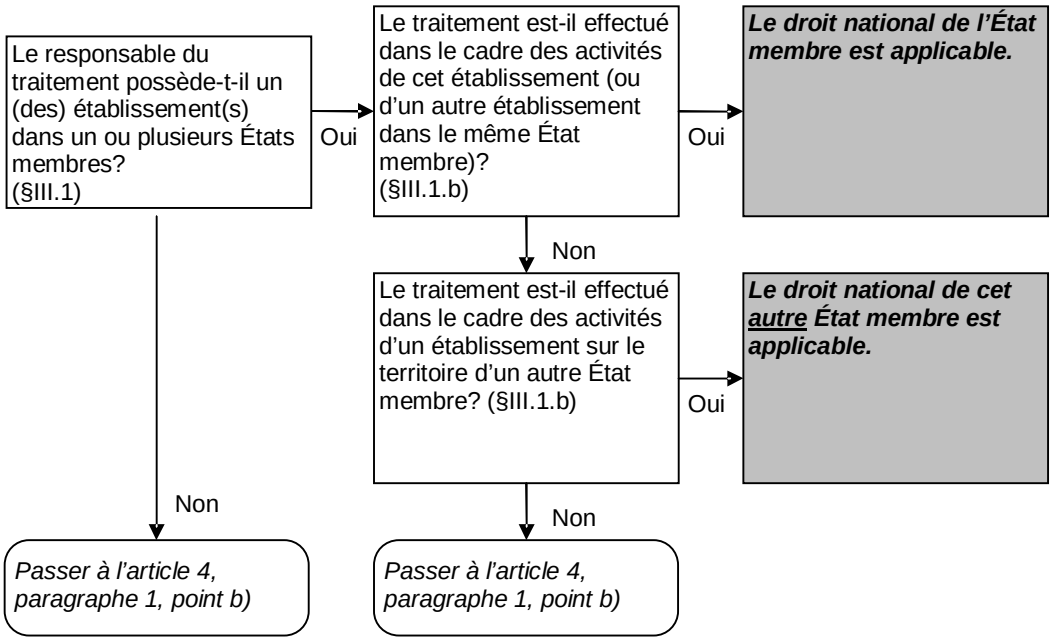
Fait à Bruxelles, le 16 décembre 2010

Pour le groupe de travail,

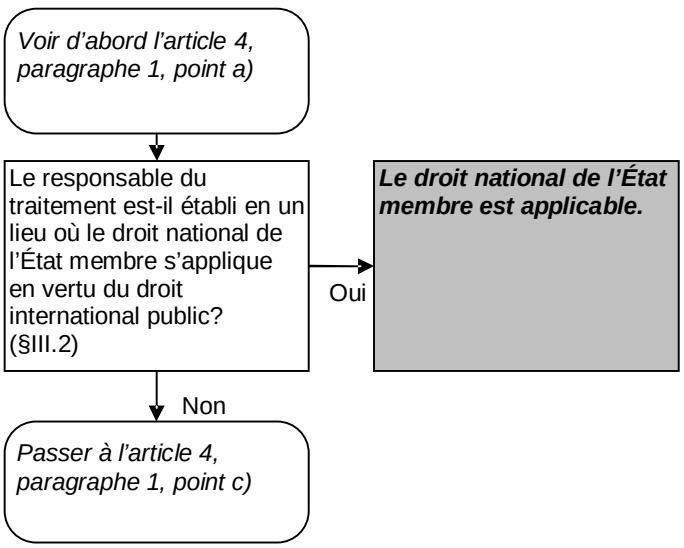
Le président
Jacob KOHNSTAMM

ANNEXE

Article 4, paragraphe 1, point a)



Article 4, paragraphe 1, point b)



Article 4, paragraphe 1, point c)