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

00530/12/FR
WP 191

Avis 01/2012 sur les propositions de réforme de la protection des données

Adopté le 23 mars 2012

Table des matières

Introduction 4
Remarques générales 5
En ce qui concerne le règlement 6
Aspects positifs 6
Rôle de la Commission 7
Rôle des autorités européennes chargées de la protection des données dans l'élaboration des politiques 8
Seuils pour les PME 9
Incidences sur le budget et les ressources 9
Dispositions générales 10
Le principe du droit d'accès du public aux informations 12
Utilisation ultérieure incompatible 13
Exceptions introduites pour les autorités publiques 13
Mineurs 14
Droit à l'oubli numérique 15
Marketing direct 15
Profilage 16
Représentant 16
Responsabilité 17
Notification des violations de données 18
En ce qui concerne le rôle et le fonctionnement des autorités chargées de la protection des données 19
Territorialité et compétence des autorités chargées de la protection des données (guichet unique) 20
Assistance mutuelle 21
Cohérence 22
«Guichet unique» pour les personnes concernées 24
Structure institutionnelle du comité européen de la protection des données 24
Transferts internationaux 25
Divulgations non autorisées par la législation de l'UE 25
Droit à réparation et responsabilité 26
Amendes 26
Recours juridictionnels 27
Églises et associations religieuses 29
En ce qui concerne la directive 29
Choix de l'instrument 29

Cohérence 29
Champ d’application 30
Principes de traitement des données 31
Droits des personnes concernées 32
Obligations des responsables du traitement 33
Transferts internationaux 34
Pouvoirs des autorités chargées de la protection des données et coopération 35
Éléments manquants 36

Introduction

Le groupe de travail «article 29» sur la protection des données (ci-après le «groupe de travail» ou le "groupe de travail «article 29»") salue les propositions adoptées par la Commission européenne dans le but de renforcer la position des personnes concernées, d'accroître la responsabilité des responsables du traitement et de consolider la position des autorités de contrôle, sur le plan tant national qu'international. Sous réserve d'améliorations à apporter, les règles proposées peuvent réduire de manière significative la fragmentation actuelle et renforcer la protection des données dans toute l'Europe.

Le groupe de travail salue en particulier l'introduction de dispositions qui encouragent les responsables du traitement à se mobiliser, dès le début, pour une protection correcte des données (au moyen, notamment, d'analyses d'impact relatives à la protection des données, d'une protection des données dès la conception et d'une protection des données par défaut). Les propositions attribuent clairement aux entités chargées du traitement des données à caractère personnel une responsabilité et une obligation de rendre compte, tout au long du cycle de vie de ces informations.

Le groupe de travail souligne l'importance des dispositions visant à clarifier et renforcer les droits des personnes concernées, notamment par la clarification de la notion de consentement, l'introduction d'un principe général de transparence et de mécanismes de recours améliorés. De même, le groupe de travail salue vivement l'instauration d'une obligation de notification des violations de données, qui assure une cohérence dans tous les secteurs.

Le groupe de travail se félicite également du fait que les propositions harmonisent les pouvoirs et compétences des autorités de contrôle afin qu'elles garantissent de manière plus efficace le respect des dispositions, et au besoin imposent ce respect, tant sur un plan individuel qu'en coopération les unes avec les autres, par exemple en ayant la capacité d'infliger des amendes importantes.

En dépit de sa position globalement positive à l'égard de la proposition de règlement, le groupe de travail estime que certaines de ses parties ont besoin d'être clarifiées et améliorées. En ce qui concerne la directive relative à la protection des données dans le domaine de la police et de la justice, le groupe de travail est déçu par le degré d'ambition de la Commission et souligne le besoin de dispositions plus fortes.

Le groupe de travail a examiné avec soin les deux propositions et livre, avec le présent avis, sa première réaction générale à leur égard. L'avis attire l'attention sur des domaines de préoccupation et, selon le cas, propose des améliorations. Au besoin, le groupe de travail pourra formuler à l'avenir d'autres avis sur des dispositions ou des aspects particuliers des propositions.

Le groupe de travail prie le Conseil et les membres du Parlement européen de saisir la possibilité qui leur est offerte d'améliorer les deux propositions pour renforcer la protection des données à caractère personnel dans l'Union européenne.

Remarques générales

Le règlement répond à l'ambition de produire un texte rendant compte de l'importance accrue de la protection des données au sein de l'ordre juridique de l'UE (article 16 du traité, article 8 de la charte). Il conserve et renforce les principes fondamentaux de la protection des données, impose des obligations claires et uniformes aux responsables du traitement et aux sous-traitants, favorise la libre circulation des données à caractère personnel et offre un cadre juridique renforcé pour que la législation soit appliquée de manière uniforme par les autorités chargées de la protection des données, dont les pouvoirs ont été consolidés.

Le groupe de travail regrette que les opinions qu'il a exprimées quant au caractère global n'aient pas donné lieu à un seul instrument juridique. Il relève que la Commission a choisi de présenter une proposition distincte de directive applicable dans le domaine de la police et de la justice pénale, en raison de contraintes politiques. Il est donc d'autant plus nécessaire de disposer d'un niveau élevé de normes cohérentes en matière de protection des données, également applicables à ce domaine. En tout état de cause, il convient de préciser que la nouvelle directive ne doit pas amener les États membres à abaisser les normes de protection des données qu'ils appliquent actuellement au secteur de la police et de la justice pénale. De même, le nouveau cadre juridique doit être conforme aux autres accords internationaux, y compris la convention 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel et son protocole additionnel. Le groupe de travail propose de mentionner clairement la convention 108 et son protocole additionnel dans le préambule du règlement et celui de la directive.

Dans de précédents avis, le groupe de travail a souligné la nécessité de parvenir à conférer un caractère global au cadre juridique. De ce point de vue, la directive est décevante en ce qu'elle manque d'ambition par rapport au règlement. Le fait que deux instruments juridiques aient été présentés ne signifie pas nécessairement qu'un cadre juridique global n'est plus possible, dès lors que le but est le même (atteindre un niveau élevé et global de protection des données pour le citoyen européen) et que les instruments ont une approche commune à l'égard, entre autres, des principes de la protection des données, des droits des personnes concernées et des obligations qui incombent aux responsables du traitement et aux sous-traitants.

Des efforts considérables doivent être déployés par le législateur européen pendant la procédure législative pour rapprocher les dispositions de fond de la directive de celles du règlement et garantir la cohérence des deux textes.

En outre, les institutions de l'UE devraient être tenues par les mêmes règles que celles qui s'appliquent au niveau des États membres. Dès lors, pour que la réforme soit véritablement globale, lors de l'entrée en vigueur du règlement, le cadre pour la protection des données propre aux institutions de l'Union européenne, tel qu'il est actuellement prévu par le règlement n° 45/2001, devra être aligné sur ce nouveau règlement.

Il en va de même pour les règles spécifiques applicables au traitement des données dans le cadre de l'ancien troisième pilier de l'UE, par exemple relativement aux agences européennes comme Europol et Eurojust. Le groupe de travail prend note des difficultés pratiques susceptibles de faire obstacle à toute proposition de remaniement général de l'acquis actuel, mais estime dans le même temps que le même niveau de protection des données devrait en

définitive s'appliquer à l'ensemble des traitements de données dans ce domaine, y compris aux organes de l'UE.

Ceci dit, le groupe de travail prend note du fait que la Commission s'est engagée à réexaminer dans un délai de trois ans d'autres instruments juridiques afin de déterminer si leur adaptation est nécessaire. Le groupe de travail recommande au législateur de fixer un délai beaucoup plus strict et demande à la Commission d'effectivement présenter ces propositions. Dans le même temps, le groupe de travail reconnaît que les régimes actuels de protection des données applicables à certains instruments et organes existants sont plus ambitieux que la directive proposée. Comme mentionné pour les États membres se trouvant dans une situation semblable, l'alignement des régimes actuels sur la directive ne devrait en aucun cas signifier un abaissement de la norme actuelle en matière de protection des données.

Dans un autre registre, le groupe de travail regrette que ni le règlement ni la directive n'abordent la question de la collecte et du transfert par des entités privées ou des autorités publiques non répressives de données en fait destinées à des fins répressives, ainsi que l'utilisation ultérieure de ces données par les autorités répressives. Plusieurs exemples survenus au cours des dix dernières années (données des dossiers passagers (PNR), rétention des données de télécommunications) ont fait clairement ressortir que des conditions strictes sont nécessaires, en particulier lorsque le traitement se fait sur une base structurelle. Il en va de même dans l'autre sens: des règles sont également nécessaires pour garantir la protection des données lorsque des informations sont transférées par les autorités répressives ou d'autres autorités «compétentes» au secteur privé ou à d'autres autorités publiques.

Enfin, en ce qui concerne les deux instruments proposés, le groupe de travail constate avec préoccupation l'étendue du pouvoir conféré à la Commission pour adopter des actes délégués et des actes d'exécution. Tout en reconnaissant qu'il est nécessaire de veiller à ce que certaines questions puissent, à un stade ultérieur, être traitées de manière plus précise, le groupe de travail estime que cela ne vaut pas, par exemple, pour les règles relatives à la notification des violations de données. Afin de garantir la sécurité juridique, il convient d'insérer les éléments essentiels dans le règlement lui-même, comme le prévoit l'article 290 du TFUE.

En ce qui concerne le règlement

Aspects positifs

- D'une manière générale, le règlement apporte davantage de clarté par des définitions plus précises et des dispositions destinées à garantir une application plus harmonisée de la législation, facilitant ainsi la libre circulation des données.

- En ce qui concerne les personnes, le règlement renforce leurs droits, y compris par une transparence accrue, un plus grand contrôle du traitement, la minimisation des données, des dispositions particulières pour le traitement des données à caractère personnel concernant des enfants, un droit d'accès aux données renforcé, un droit d'opposition renforcé, le droit à la portabilité des données, un droit à la suppression des données renforcé («droit à l'oubli numérique») et un droit renforcé de recours devant les autorités chargées de la protection des données et devant les cours et tribunaux.

- En ce qui concerne les responsables du traitement, le règlement apporte une simplification et une plus grande cohérence, un recentrage sur leur responsabilité à l'égard des données traitées et la nécessité de prouver cette responsabilisation par une protection des données dès la conception, une protection des données par défaut, des analyses d'impact sur le respect de la vie privée, la désignation d'un délégué à la protection des données, des obligations liées à la notification des violations de données et l'adoption de mesures de précaution à l'égard des transferts internationaux. En outre, les règles d'entreprise contraignantes sont expressément reconnues comme un outil permettant d'encadrer les transferts internationaux.

- •En ce qui concerne les sous-traitants, les obligations en matière de sécurité des données sont juridiquement fondées, et une obligation a été introduite pour que le sous-traitant endosse la responsabilité du responsable du traitement à l'égard d'une opération spécifique de traitement de données au cas où il outrepasserait les instructions du responsable du traitement à propos de ladite opération de traitement (cela présente de l'intérêt pour les prestataires «cloud»).

- En ce qui concerne les autorités chargées de la protection des données, le règlement prévoit une indépendance et des pouvoirs renforcés, y compris des amendes administratives et l'obligation de consulter ces autorités à propos des mesures législatives, et il comprend des dispositions visant à garantir une application harmonisée de la législation et, au besoin, son application forcée, en particulier au moyen du «mécanisme de contrôle de la cohérence».

Rôle de la Commission

Le groupe de travail émet de sérieuses réserves à l'égard de l'étendue du pouvoir conféré à la Commission pour adopter des actes délégués et des actes d'exécution, ce qui est tout particulièrement pertinent au vu du fait qu'il est question d'un droit fondamental. Naturellement, il peut être nécessaire de laisser certaines questions à des actes délégués et/ou d'exécution. Toutefois, toutes les questions mentionnées à l'article 86 et à l'article 87 ne constituent pas des points de détail. Certaines dispositions du règlement (par exemple, sur la notification des violations de données, l'assistance mutuelle, la cohérence et la dérogation au droit d'information et d'accès dans le cadre d'un traitement à des fins historiques, statistiques et scientifiques) ne peuvent être appliquées sans que l'acte délégué ou d'exécution soit en vigueur. De plus, d'autres actes délégués concernent le champ d'application matériel du règlement, par exemple l'article 6, paragraphe 1, point f), lu conjointement avec l'article 6, paragraphe 5, qui permet à la Commission de définir les «intérêts légitimes» du responsable du traitement dans des situations particulières de traitement et des secteurs donnés. Afin de garantir la sécurité juridique, il faut insérer les éléments essentiels dans le règlement lui-même, comme le prévoit l'article 290 du TFUE.

Dans la pratique, l'adoption d'actes délégués ou d'actes d'exécution pour un grand nombre d'articles peut prendre plusieurs années et pourrait représenter une insécurité juridique pour les responsables du traitement et les sous-traitants qui espèrent une mise en œuvre rapide et obtenir des lignes directrices concrètes à bref délai. Le groupe de travail prie la Commission d'indiquer à tout le moins quels sont les actes délégués et d'exécution qu'elle compte adopter à court, moyen et long terme.

En dépit du rôle de gardienne des traités dévolu à la Commission, le groupe de travail émet également de sérieuses réserves quant au rôle attribué à la Commission dans les cas particuliers examinés dans le cadre du mécanisme de contrôle de la cohérence, puisqu'il empiète sur l'indépendance des autorités chargées de la protection des données. Lorsqu'une question est examinée ou a été examinée par le comité européen de la protection des données dans le cadre du mécanisme de contrôle de la cohérence, la Commission devrait être en mesure de donner son appréciation juridique tout en s'abstenant en principe d'intervenir. Une procédure pourrait être envisagée pour permettre à la Commission et au comité européen de la protection des données de demander à la Cour de justice de l'Union européenne d'émettre un avis sur l'interprétation du règlement.

Rôle des autorités européennes chargées de la protection des données dans l'élaboration des politiques

Le groupe de travail estime que les propositions devraient refléter le rôle important qu'il a lui-même joué jusqu'à présent et celui que le comité européen de la protection des données est susceptible de jouer dans le futur en termes d'élaboration des politiques (par exemple, en formulant des lignes directrices ou des recommandations).

À l'article 66, il est prévu que le comité européen de la protection des données, de sa propre initiative ou à la demande de la Commission, a pour mission de conseiller sur toute question relative à la protection des données à caractère personnel et d'examiner toute question portant sur l'application du règlement. Le groupe de travail entend cette disposition comme incluant également d'autres instruments législatifs et suggère dès lors d'ajouter à l'article 66, paragraphe 1, point a), «[...] ainsi que sur toute mesure additionnelle ou particulière visant à garantir les droits et libertés des personnes physiques à l'égard du traitement des données à caractère personnel et sur toute autre proposition de mesure de l'Union affectant lesdits droits et libertés».

De plus, le groupe de travail suggère d'introduire la possibilité pour la Commission européenne mais aussi pour le Parlement européen de solliciter l'avis du comité européen de la protection des données en ajoutant les termes «et du Parlement européen» à l'article 66, paragraphe 1, point b).

En outre, le groupe de travail suggère vivement d'inclure l'obligation pour la Commission de toujours consulter le comité européen de la protection des données au sujet des décisions relatives au caractère adéquat du niveau de protection (article 41) et des clauses types de protection des données (article 42), et de consulter et obtenir l'approbation dudit comité au sujet des codes de conduite au niveau européen (article 38). En tout état de cause, il convient d'insérer une obligation faite à la Commission de consulter le comité européen de la protection des données au sujet de tous les actes délégués et d'exécution (articles 86 et 87).

Les autorités nationales devraient continuer à pouvoir formuler des lignes directrices et des recommandations devant être soumises au mécanisme de contrôle de la cohérence si celles-ci risquent d'avoir une incidence importante sur d'autres États membres. Elles devraient également pouvoir contrôler l'élaboration des marques et labels de certification destinés à protéger les personnes.

Seuils pour les PME

Le groupe de travail relève que tout au long de la proposition de règlement, des exceptions et seuils sont introduits dans le but de limiter les charges administratives des micro, petites et moyennes entreprises et d'atténuer les conséquences pour celles-ci. Des seuils sont introduits dans les dispositions concernant l'obligation de désigner un représentant dans l'UE (article 25), la documentation (article 28, paragraphe 4), la désignation d'un délégué à la protection des données (article 35, paragraphe 1) et les amendes administratives (articles 79, paragraphe 3). De surcroît, la proposition prévoit des actes délégués et d'exécution autorisant la Commission à prendre d'autres mesures pour les micro, petites et moyennes entreprises à l'article 12, paragraphe 6, sur les procédures et mécanismes prévus pour l'exercice des droits de la personne concernée, à l'article 14, paragraphe 7, sur l'obligation d'informer la personne concernée, à l'article 22, paragraphe 4, sur les obligations de rendre compte et à l'article 33, paragraphe 6, sur les analyses d'impact relatives à la protection des données.

Le groupe de travail est d'avis que les personnes concernées devraient bénéficier du même niveau de protection, que leurs données soient traitées par une micro, petite, moyenne entreprise ou une grande entreprise. Toutefois, il reconnaît que certaines des obligations envisagées pourraient être pesantes pour les micro, moyennes et petites entreprises. Dès lors, si le groupe de travail comprend le principe qui justifie d'introduire ces seuils, il craint que ces exceptions n'aboutissent, dans la pratique comme en ce qui concerne la protection des données à caractère personnel, à des effets incohérents et des résultats non souhaitables. Le groupe de travail estime qu'un seuil tenant compte de la nature et de l'étendue du traitement des données serait plus approprié.

Incidences sur le budget et les ressources

Le groupe de travail se réjouit de ce que les propositions reconnaissent le rôle important susceptible d'être joué par les autorités chargées de la protection des données pour assurer le respect de l'instrument, en attribuant des fonctions renforcées à la fois à ces autorités et au comité européen de la protection des données. Le groupe de travail doute toutefois sérieusement que l'incidence budgétaire considérable de ces fonctions renforcées soit suffisamment reconnue. Pour permettre aux autorités chargées de la protection des données et au comité européen de la protection des données de s'acquitter efficacement de leurs fonctions, y compris en termes d'assistance mutuelle et de coopération au sein du mécanisme de contrôle de la cohérence, les États membres doivent s'engager à fournir les ressources financières, humaines et techniques nécessaires.

À cet égard, le groupe de travail suggère vivement qu'une évaluation approfondie indépendante soit réalisée concernant les coûts supplémentaires que cela représente pour les autorités chargées de la protection des données et le contrôleur européen de la protection des données (en tant que secrétariat du comité européen de la protection des données), sur la base des propositions actuelles. Eu égard aux résultats de cette évaluation, il conviendrait de préciser ce que constituent pour les autorités chargées de la protection des données les «ressources humaines, techniques et financières appropriées, ainsi que [les] locaux et [...] l'infrastructure» mentionnés à l'article 47, paragraphe 5.

Le groupe de travail compte adresser un courrier séparé à la Commission au sujet de la finalité et des paramètres d'une analyse d'impact de ce type.

Dispositions générales

Champ d'application

Conformément à l'article 3, paragraphe 2, le règlement s'applique également au traitement des données à caractère personnel relatives à des personnes concernées ayant leur résidence sur le territoire de l'Union, par un responsable du traitement qui n'est pas établi dans l'Union, lorsque les activités de traitement sont liées à l'offre de biens ou de services à ces personnes concernées dans l'Union ou à l'observation de leur comportement.

En dépit des tentatives de définition des expressions «offre de biens et de services» et «observation de leur comportement» dans les considérants, le groupe de travail estime qu'il serait utile de clarifier davantage ces notions.

Il devrait être précisé que l'«offre de biens et de services» comprend également les services gratuits (dans le cadre desquels les personnes paient en fait le service en fournissant leurs données à caractère personnel). Le groupe de travail propose dès lors d'ajouter une formule du genre «y compris des services fournis sans qu'aucune contrepartie financière ne soit exigée de la personne».

En outre, le considérant 21 laisse entendre que l'«observation [du] comportement» est liée à un suivi sur l'internet et à la création de profils. Le groupe de travail recommande de modifier le libellé afin de garantir que même si le responsable du traitement ne crée pas de profils en tant que tels, les activités de traitement puissent parfois être considérées comme une «observation du comportement» si elles donnent lieu à des décisions à propos d'une personne concernée ou impliquent d'analyser ou de prévoir ses préférences personnelles, ses comportements et ses attitudes.

Personne concernée et données à caractère personnel

Le groupe de travail salue la définition de la «personne concernée» donnée à l'article 4, point 1, de la proposition de règlement, qui dispose: «"personne concernée": une personne physique identifiée ou une personne physique qui peut être identifiée [...]». On peut considérer qu'une personne physique est identifiable lorsque, au sein d'un groupe de personnes, elle peut être distinguée des autres membres du groupe et, par conséquent, être traitée différemment. C'est ce qui a été exposé dans l'avis sur le concept de données à caractère personnel précédemment adopté par le groupe de travail (WP 136). Il convient donc de modifier le considérant 23 afin de préciser que la notion de caractère identifiable comprend également le fait d'être distinguable de cette manière.

Le considérant 24 relatif à la définition des données à caractère personnel prévoit que les numéros d'identification, données de localisation, identifiants en ligne ou autres éléments spécifiques ne doivent pas nécessairement être considérés comme des données à caractère personnel dans tous les cas de figure. Telle qu'elle est rédigée actuellement, la dernière phrase pourrait donner lieu à une interprétation indûment restrictive de la notion de données à caractère personnel en ce qui concerne, par exemple, les adresses IP ou les témoins de connexion («cookies»). Le groupe de travail rappelle que les données à caractère personnel sont des données concernant une personne identifiable. «Les données concernent une personne si elles ont trait à l'identité, aux caractéristiques ou au comportement d'une personne ou si cette information est utilisée pour déterminer ou influencer la façon dont cette

personne est traitée ou évaluée»[1]. Le groupe de travail a déjà présenté, dans l'avis WP 136, différents scénarios qui justifieraient de considérer que les adresses IP se rapportent à des personnes identifiables, «notamment [...] lorsque le traitement d'adresses IP [a] été effectué pour identifier les utilisateurs de l'ordinateur (par exemple, par des titulaires de droits d'auteur afin de poursuivre ces utilisateurs d'ordinateurs pour violation de droits de la propriété intellectuelle) [...]». Dans ce cas, de même que dans celui des cookies, le responsable du traitement part du principe que des «moyens susceptibles d'être raisonnablement mis en œuvre» seront disponibles pour identifier les personnes et les traiter d'une manière particulière[2]. Dès lors, le groupe de travail suggère de modifier en conséquence le considérant 24.

Données biométriques

Le groupe de travail salue l'introduction d'une définition des données biométriques à l'article 4, point 11, du règlement. Néanmoins, il émet des réserves quant au libellé actuel, qui s'attache au fait de permettre l'identification unique d'une personne. Les données biométriques ne sont pas uniquement utilisées à des fins d'identification, mais également dans un but d'authentification (pour vérifier l'identité d'une personne sans en fait identifier la personne elle-même). Il conviendrait de modifier la définition pour l'axer sur les types de données qui doivent être considérées comme des données biométriques plutôt que sur ce que ces données permettent de faire. Le groupe de travail suggère dès lors de modifier le libellé de l'article 4, point 11, en remplaçant «[...] permettent son identification unique [...]» par «[...] sont uniques pour chaque personne en particulier [...]».

Établissement principal

Il faut davantage clarifier la manière dont il est décidé du lieu où une entreprise multinationale (que ses propriétaires soient établis ou non dans l'UE) a son établissement principal, tel que ce terme est défini à l'article 4, point 13, et au considérant 27, y compris lorsqu'elle comprend des entités juridiques distinctes actives dans différents secteurs. À titre d'exemple, il pourrait être tenu compte de l'«influence dominante» exercée par un établissement sur les opérations de traitement en ce qui concerne l'application des règles relatives à la protection des données à caractère personnel.

Le groupe de travail relève que la proposition de règlement comporte, à l'article 4, différentes définitions d'entités économiques, qui ne sont pas clairement distinctes les unes des autres. Les notions de «responsable du traitement» et d'«établissement principal», d'une part, renvoient au lieu où sont prises les décisions importantes concernant le traitement des données, tandis que les définitions d'«entreprise» et de «groupe d'entreprises», d'autre part, parlent de l'activité économique et de la structure de l'entreprise.

Un terme supplémentaire est introduit en ce qui concerne les sous-traitants dont l'établissement principal est censé être le lieu de leur «administration centrale». En outre, le chapitre VIII sur les recours, la responsabilité et les sanctions mentionne un établissement, quel qu'il soit, lorsqu'il s'agit de déterminer la juridiction compétente pour intenter une action contre un responsable du traitement ou un sous-traitant, indépendamment du fait que ledit établissement ait un lien quelconque avec le traitement en question (il pourrait en effet être,

1 WP 136, p. 10.
2 WP 136, p. 16.

d'un point de vue juridique, complètement indépendant des autres établissements du responsable du traitement/sous-traitant établis dans l'UE).

De l'avis du groupe de travail, ces définitions se chevauchent et devraient dès lors faire l'objet d'une clarification. En tout état de cause, il conviendrait de préciser quel est le lien entre l'établissement principal et les responsabilités du responsable du traitement.

La définition de l'établissement principal semble essentiellement destinée à déterminer quelle est l'autorité nationale chargée de la protection des données qui doit être l'autorité chef de file dans un cas particulier ou pour une entreprise donnée. Il est essentiel que le terme «établissement principal» soit clairement compris, puisqu'il est décisif pour déterminer l'autorité chef de file au sens de l'article 51, paragraphe 2, lorsque le traitement des données à caractère personnel a lieu dans le cadre des activités d'un responsable du traitement ou d'un sous-traitant établis dans l'Union, et lorsque le responsable du traitement ou le sous-traitant sont établis dans plusieurs États membres (voir page 30 pour de plus amples détails).

Pseudonymisation

Le groupe de travail estime que la notion de pseudonymisation devrait être introduite de manière plus explicite dans l'instrument (par exemple, en intégrant une définition des données pseudonymisées, cohérente avec la définition des données à caractère personnel), car elle peut permettre d'accéder à une meilleure protection des données, comme dans le cadre de la protection des données dès la conception et de la protection des données par défaut. Le groupe de travail suggère dès lors d'instaurer une obligation générale d'anonymisation ou de pseudonymisation des données à caractère personnel dans la mesure de ce qui est possible et proportionné par rapport à la finalité du traitement. Ce principe pourrait être introduit à l'article 5 et, dans le cadre de la protection des données dès la conception et par défaut, à l'article 23.

Protection des données dès la conception et protection des données par défaut

Le groupe de travail salue l'introduction à l'article 23 de la protection des données dès la conception et de la protection des données par défaut, mais recommande de clarifier le sens de ces notions dans un considérant, par exemple, en indiquant que les fonctions respectueuses de la vie privée devraient être automatiquement activées sur les biens et services et que des procédures adéquates devraient être mises en œuvre pendant la conception du traitement des données ou du produit. Naturellement, il appartient au responsable du traitement de prouver que ses activités de traitement tiennent compte des notions de protection des données dès la conception et de protection des données par défaut, qui constituent des mesures appropriées au sens de l'article 22, paragraphe 1.

Le groupe de travail note que la Commission est habilitée à définir des normes techniques en la matière. Le groupe de travail est convaincu que la Commission devrait associer le comité européen de la protection des données et des organismes de normalisation internationaux à l'élaboration de ces normes techniques, et le cas échéant les consulter.

<u>Le principe du droit d'accès du public aux informations</u>

Le considérant 18 prévoit que le règlement permet de prendre en compte, dans la mise en œuvre de ses dispositions, le principe du droit d'accès du public aux documents

administratifs. Ce principe constituant de longue date un droit fondamental important, il devrait être mentionné dans un considérant, mais également exprimé dans un article du règlement.

Utilisation ultérieure incompatible

L'article 6, paragraphe 4, introduit la possibilité d'un traitement ultérieur des données à des fins non compatibles lorsque ledit traitement peut trouver une autre base juridique (à l'exception de l'intérêt légitime du responsable du traitement). Si le groupe de travail ne conteste pas la nécessité de laisser ouverte la possibilité d'un traitement ultérieur des données à d'autres fins, la disposition telle qu'elle est actuellement proposée crée les conditions d'une utilisation ultérieure des données à des fins non compatibles qui pourraient, dans le secteur tant public que privé, en particulier si elles se fondent sur les points b) (exécution d'un contrat) et e) (intérêt général), donner lieu à des résultats extrêmement peu souhaitables. De l'avis du groupe de travail, cette disposition va à l'encontre du principe général de limitation de la finalité, l'une des notions clés de la protection des données en Europe, et suggère donc vivement soit de supprimer l'article 6, paragraphe 4, soit de le reformuler, d'une manière plus précise avec un renvoi à l'article 21. Dans ce contexte, le groupe de travail souhaite également attirer l'attention sur le fait qu'il abordera la question de l'utilisation compatible de manière plus substantielle dans un avis distinct dans le courant de 2012, comme indiqué dans son programme de travail pour 2012-2013.

Exceptions introduites pour les autorités publiques

L'une des raisons qui motivent la révision du cadre régissant la protection des données est de garantir son caractère global. En offrant un ensemble unique de règles applicables tant par le secteur public que privé, le cadre juridique devrait améliorer la sécurité juridique à l'égard des garanties offertes en matière de protection des données dans les différents secteurs, en particulier pour les personnes physiques.

Le groupe de travail a déjà fait part de sa déception quant au manque d'ambition dans le domaine de la police et de la justice. Toutefois, dans le règlement lui-même, une position particulière est également accordée au secteur public. Le groupe de travail s'inquiète du fait qu'en plusieurs endroits du règlement, de larges exceptions en faveur des autorités publiques soient introduites pour des motifs d'intérêt général. Le groupe de travail estime que des exceptions larges et indéterminées, qui ne présentent pas non plus les garanties adéquates pour la protection des personnes, ne sont pas justifiées. Dès lors, il suggère de définir autant que possible dans le règlement les intérêts généraux spécifiques. Cela contribuerait également à une harmonisation au sein de l'UE.

Comme mentionné ci-dessus, l'article 6, paragraphe 4, introduit pour les autorités publiques également la très large possibilité de remplacer la finalité initiale du traitement par des finalités non compatibles. En outre, l'article 9, paragraphe 2, point g), permet le traitement de données sensibles pour des missions effectuées «dans l'intérêt général». Il en va de même pour les exceptions formulées à l'article 17, paragraphe 5, en particulier en ce qui concerne l'intérêt général et les intérêts de tiers. Le groupe de travail recommande de limiter cette exception selon les termes suivants: «[...] pour des motifs d'intérêt général important».

En outre, l'article 21 prévoit la possibilité de limiter les principes de protection des données et les droits des personnes concernées, élargissant ainsi les possibilités de limitation par rapport à la situation actuelle, sans prévoir les garanties adéquates à respecter lorsque l'article est invoqué. De plus, l'article 21, paragraphe 1, point c), peut être invoqué pour sauvegarder une catégorie ouverte d'«autres intérêts généraux». Le groupe de travail juge ces possibilités trop vastes et suggère donc vivement de supprimer les termes «sauvegarder d'autres intérêts généraux de l'Union ou d'un État membre [...]» de l'article 21, paragraphe 1, point c), et de commencer par «[...] un intérêt économique ou financier important [...]».

L'article 33, paragraphe 5, introduit pour les autorités publiques une dérogation à l'obligation d'effectuer des analyses d'impact relatives à la protection des données lorsque le traitement est effectué en exécution d'une obligation légale. Le groupe de travail est d'avis que la seule dérogation qui pourrait être justifiée dans ce contexte serait le cas dans lequel une analyse d'impact relative à la protection des données aurait déjà été effectuée dans le cadre de la procédure législative.

Le groupe de travail est convaincu que des exceptions générales pour le secteur public ne sont pas justifiées et qu'elles portent préjudice au caractère global du cadre juridique; il recommande vivement que, dans la mesure du possible, les secteurs public et privé soient traités de la même manière et tenus de respecter le même ensemble de règles de base. Toutefois, il faut également empêcher que le nouveau cadre juridique puisse entraîner un affaiblissement du niveau de protection des données déjà atteint dans différents domaines dans les États membres. Dans le secteur public en particulier, le niveau de protection des données varie du fait des pratiques et évolutions constitutionnelles et juridiques. Le nouveau cadre juridique devrait dès lors prévoir un niveau élevé et harmonisé de normes dans ce domaine, tout en offrant aux États membres la possibilité d'apporter d'autres précisions (comme le prévoit déjà le chapitre IX), mais sans préjudice du règlement. Cela signifie également qu'elles pourraient compléter le règlement.

Mineurs

Le groupe de travail reconnaît l'importance du principe de l'«intérêt supérieur de l'enfant» et de la notion de protection progressive en fonction du degré de maturité[3]. Bien que le règlement n'affecte pas les dispositions régissant la validité, la formation ou les effets d'un contrat à l'égard d'un enfant figurant dans la législation générale des États membres en matière contractuelle, le groupe de travail salue le fait que l'article 8, paragraphe 1, prévoie que, s'agissant de l'offre directe de services de la société de l'information aux enfants, le traitement des données à caractère personnel relatives à un enfant de moins de 13 ans n'est licite que si et dans la mesure où le consentement est donné ou autorisé par un parent de l'enfant ou par une personne qui en a la garde.

Le groupe de travail est attentif aux contraintes relatives à l'harmonisation des limites d'âge dans un tel instrument et comprend que dans des situations purement nationales, le droit des États membres devrait s'appliquer. Toutefois, le groupe de travail suggère d'élargir à des domaines autres que l'offre de services de la société de l'information la portée de la norme minimale introduite dans le règlement en ce qui concerne la manière dont sont traités les

[3] Voir l'avis 2/2009 sur la protection des données à caractère personnel de l'enfant (WP 160) et le document de travail 1/2008 sur la protection des données à caractère personnel de l'enfant (WP 147).

mineurs, puisqu'il existe davantage de situations dans lesquelles des règles spécifiques pourraient être envisagées.

D'une manière générale, le règlement manque de dispositions relatives à la manière dont des droits peuvent être exercés par le biais d'une représentation par des avocats, non seulement dans le cas des mineurs mais également des personnes incapables.

Droit à l'oubli numérique

Le groupe de travail salue l'inclusion spécifique dans le règlement du droit à l'oubli numérique et à l'effacement en tant que moyen permettant de renforcer le contrôle exercé par les personnes sur leurs propres données à caractère personnel. Toutefois, la façon dont ces droits sont configurés par le règlement et la manière dont l'internet fonctionne dans la réalité pourraient considérablement limiter leur efficacité.

Le responsable du traitement est chargé, non seulement, d'effacer les données mais également d'informer de la demande de la personne concernée les tiers qui traitent ces données par le biais de liens vers celles-ci, de copies ou de reproductions de celles-ci. Le fait de faire porter cette obligation au seul responsable du traitement comporte des limites, puisqu'il peut y avoir des situations dans lesquelles le responsable du traitement a pris toutes les mesures raisonnables pour informer les tiers, mais n'a pas connaissance de toutes les copies ou reproductions existantes ou des nouvelles copies ou reproductions qui apparaissent après qu'il a informé tous les tiers connus. Mais surtout, aucune disposition du règlement ne semble obliger les tiers à respecter la demande formulée par la personne concernée, à moins que ces tiers ne soient également considérés comme responsables du traitement.

Le règlement n'indique aucunement comment les personnes concernées peuvent exercer leurs droits si le responsable du traitement n'existe plus, a disparu ou ne peut être identifié ou contacté. Dès lors, la position des tiers qui traitent des données devrait être clarifiée afin de définir dans quelles conditions et à quel titre ils doivent exécuter la demande de la personne concernée, et quelles sont les conséquences s'ils ne le font pas.

De la même façon, on pourrait envisager d'élargir le droit des personnes concernées pour leur permettre d'adresser leur demande d'effacement directement aux tiers dans le cas où cela ne peut être fait par le biais du responsable du traitement.

Pour finir, aucun mécanisme ne prévoit la suppression des copies ou reproductions des données ou des liens vers les données qui ne sont pas effacées conformément à l'article 17, paragraphe 3, mais qui, en soi, ne relèvent pas des motifs exposés dans l'article. Or ces liens, copies ou reproductions peuvent faciliter l'accès au contenu d'origine, alors que cela ne se justifie pas forcément en vertu dudit article. Naturellement, le groupe de travail reconnaît la nécessité de trouver le juste équilibre entre les droits relatifs au respect de la vie privée et le droit à la liberté d'expression. Il conviendrait que le règlement clarifie la relation entre l'article 17, paragraphe 3, et l'obligation formulée à l'article 17, paragraphe 2.

Marketing direct

Nonobstant l'article 19, paragraphe 2, du règlement qui prévoit un droit d'opposition au traitement des données en vue d'un marketing direct, le groupe de travail souligne que les

dispositions de la directive 2002/58/CE demeurent pleinement applicables, comme le prévoit également l'article 89 du règlement. Cela s'applique tout spécialement dans le contexte de la publicité comportementale en ligne et du marketing par courrier électronique, pour lesquels un consentement est prévu.

Profilage

Le groupe de travail soutient la disposition du règlement qui traite du profilage. Toutefois, il a des doutes quant au fait que l'approche adoptée puisse être suffisante pour tenir compte des questions de création et d'utilisation de profils, en particulier dans l'environnement en ligne. De plus, le groupe de travail relève que les termes «l'affectant de manière significative» employés à l'article 20, paragraphe 1, sont imprécis. Il conviendrait de préciser qu'il couvre également l'utilisation, par exemple, d'outils d'analyse web, le suivi pour évaluer le comportement de l'utilisateur, la création de profils de déplacement par les applications mobiles, ou la création de profils personnels par les réseaux sociaux.

En outre, la disposition ne devrait pas être limitée au traitement exclusivement automatisé mais également couvrir les méthodes de traitement partiellement automatisé. De l'avis du groupe de travail, il faudrait aborder la question en définissant clairement les fins auxquelles des profils sont susceptibles d'être créés et utilisés, y compris l'obligation spécifique incombant aux responsables du traitement d'informer la personne concernée, en particulier de son droit d'opposition à la création et utilisation de profils.

Représentant

Le groupe de travail estime que le rôle et les obligations du représentant tel qu'ils sont définis à l'article 25 devraient être davantage clarifiés. Il conviendrait de préciser quel est le rôle du représentant à l'égard des personnes concernées, des juridictions et des autorités chargées de la protection des données, en particulier au vu du fait que l'article 79, paragraphe 6, point f), prévoit l'amende la plus élevée possible en cas de non-désignation d'un représentant. Le mandat du représentant devrait être spécifié afin de définir clairement l'étendue de sa mission, son rôle et sa responsabilité.

L'article 78, paragraphe 2, prévoit que lorsque le responsable du traitement a désigné un représentant, les sanctions sont appliquées au représentant. Il conviendrait d'apporter la même clarté dans le cas des sanctions administratives prévues à l'article 79. Les termes «devrait pouvoir être contacté par toute autorité de contrôle» et «peut être contactée à sa place par les autorités de contrôle» utilisés au considérant 63 et à l'article 4, paragraphe 14, ne sont pas suffisamment précis quant au fait qu'un représentant peut également être le destinataire d'une sanction administrative au sens de l'article 79.

Il devrait également être bien clair que l'établissement d'un représentant dans l'UE, tel que visé à l'article 25, paragraphe 3 («est établi dans l'un des États membres») **ne** déclenche **pas** le mécanisme relatif à l'établissement principal défini à l'article 4, paragraphe 13, au sens où il **ne** joue **pas** un rôle **décisif** dans la détermination d'une autorité chef de file chargée de la protection des données conformément à l'article 51, paragraphe 2.

En ce qui concerne les dérogations à l'obligation de désignation d'un représentant, le groupe de travail ne voit aucune raison importante d'exclure un responsable du traitement établi dans un pays tiers qui offre un niveau de protection adéquat. Le fait qu'un pays tiers présente un niveau de protection adéquat ne modifie en rien la nécessité d'avoir un point de contact dans

l'Union européenne, et le groupe de travail suggère dès lors de supprimer l'article 25, paragraphe 2, point a).

S'il y a lieu de prévoir des dérogations à l'obligation de désignation d'un représentant, celles-ci devraient se baser sur la nature et l'étendue du traitement des données à caractère personnel, ainsi que sur le nombre (potentiel) de personnes concernées affectées dans l'UE. Le seuil actuel concernant le nombre de personnes employées par le responsable du traitement risque d'exclure des entités de petite taille dont les activités de traitement représentent un risque pour les particuliers. De même, en dépit de l'explication donnée au considérant 64, la formulation «n'offrant **qu'occasionnellement** des biens ou des services à des personnes concernées» est trop vague et pourrait, dans la pratique, trop souvent donner lieu à une interprétation erronée.

Responsabilité

Le groupe de travail accueille très favorablement l'introduction du principe de responsabilité dans le règlement, en particulier à l'article 22, et souscrit pleinement à l'objectif de mettre en place des procédures et mécanismes efficaces ciblant les traitements susceptibles de présenter des risques particuliers pour les droits et libertés des personnes concernées. Néanmoins, le groupe de travail émet quelques doutes quant aux articles qui visent à préciser le principe général.

Tout d'abord, il faut veiller à la modularité. Dans la mise en œuvre du principe de responsabilité, il devrait être possible de tenir compte de la taille du responsable du traitement et de la nature des activités de traitement. En outre, les autorités de contrôle devraient pouvoir tenir compte des mécanismes de responsabilité mis en œuvre lorsqu'elles infligent des sanctions et amendes.

De plus, l'article 28 prévoit l'obligation pour le responsable du traitement de conserver une trace documentaire de tous les traitements effectués sous sa responsabilité. L'article 28, paragraphe 2, précise le type de documentation spécifique que cela implique. Cette obligation s'articule avec les obligations générales de responsabilité énoncées à l'article 22, en vertu duquel les responsables du traitement sont tenus d'*être à même de démontrer* quelles sont les règles internes adoptées et les mesures mises en œuvre pour garantir le respect du règlement. En principe, chaque responsable du traitement, chaque sous-traitant et, le cas échéant, le représentant du responsable du traitement devraient être tenus de conserver la documentation principale relative à leurs activités de traitement de données.

Si le groupe de travail salue l'obligation d'effectuer une analyse d'impact relative à la protection des données, comme le prévoit l'article 33, il estime que cette analyse devrait naturellement être aussi réalisée lorsque l'on ne peut savoir avec certitude si le traitement est susceptible de présenter des risques particuliers pour les droits et libertés des personnes concernées. Dès lors, le groupe de travail suggère d'aligner l'article 33, paragraphe 1, sur le considérant 70 et propose d'ajouter «sont susceptibles de», de manière à ce que la première phrase de l'article soit libellée ainsi: «Lorsque les traitements **sont susceptibles de** présenter des risques particuliers [...]».

Le groupe de travail estime que les dérogations prévues à l'article 28, paragraphe 4, point b), sur la documentation et l'article 35, paragraphe 1, point b), sur la désignation des délégués à la protection des données sont susceptibles d'avoir des conséquences non voulues, en

particulier lorsqu'une entité de petite taille comptant moins de 250 salariés traite beaucoup de données à caractère personnel ou que le traitement est de nature risquée. De même, le libellé actuel a une incidence disproportionnée sur les entités de grande taille qui traitent un nombre limité de données à caractère personnel. Le groupe de travail estime qu'au lieu d'indiquer le nombre total de salariés d'une entreprise, il serait plus approprié de tenir compte de la nature et de l'étendue du traitement des données à caractère personnel, ainsi que du nombre de salariés directement associés au traitement des données à caractère personnel et/ou du nombre de personnes concernées.

Le groupe de travail estime que les traitements portant sur les catégories de données sensibles indiquées à l'article 9 du règlement devraient faire l'objet d'une analyse d'impact relative à la protection des données. Dès lors, tous les types de données sensibles devraient être repris à l'article 33, paragraphe 2, point b).

De plus, il conviendrait de supprimer la restriction introduite par l'expression «à grande échelle» en ce qui concerne les traitements mentionnés à l'article 33, paragraphe 2, points b), c) et d), car le groupe de travail estime qu'une analyse d'impact relative à la protection des données est requise pour les traitements de ce type, même à petite échelle.

Cela vaut tout particulièrement en ce qui concerne le traitement des données biométriques, qui, de l'avis du groupe de travail, devrait être considéré comme risqué dans certaines circonstances, et une analyse d'impact relative à la protection des données devrait dès lors être effectuée indépendamment d'un quelconque seuil prévu à l'article 33. De même, comme mentionné plus haut, la dérogation, à l'article 33, paragraphe 5, dispensant les autorités publiques d'effectuer une analyse d'impact n'est pas justifiée, à moins que ladite analyse n'ait déjà été effectuée lors de la procédure législative.

Notification des violations de données

Le groupe de travail salue l'introduction de l'obligation de notification d'une violation de données à caractère personnel, qui assure une cohérence dans tous les secteurs. Néanmoins, le groupe de travail doute que l'obligation de notification puisse donner lieu à des résultats satisfaisants au vu de la manière dont elle est établie. La portée de l'obligation de notification à l'autorité de contrôle devrait notamment être davantage ciblée et limitée. Il faudrait éviter que les autorités de contrôle soient dérangées et surchargées par le traitement de notifications de violations mineures de données, risquant peu de porter atteinte aux droits des personnes concernées. En outre, il faut clarifier le rôle et les responsabilités des autorités chargées de la protection des données en cas de notification (et après celle-ci).

Le groupe de travail est attentif au fait que, dans certaines circonstances, il peut être impossible d'adresser une notification dans un délai de 24 heures. L'article 31, paragraphe 1, répond à cette question en offrant la possibilité d'adresser la notification plus de 24 heures après avoir eu connaissance de la violation. Il est néanmoins important de faire la notification en temps utile. Le groupe de travail propose donc d'adopter une approche en deux étapes, selon laquelle le responsable du traitement doit en principe adresser la notification de la violation dans un délai de 24 heures après en avoir eu connaissance. Si toutes les informations ne peuvent être fournies dans le délai de 24 heures, le responsable du traitement aura la possibilité de compléter la notification dans un second temps.

Il faut apporter de plus amples précisions en ce qui concerne le critère utilisé pour établir une violation de données à caractère personnel et les circonstances dans lesquelles une violation doit être notifiée à l'autorité chargée de la protection des données et aux personnes concernées visées par la violation (par exemple, s'il y a un risque de danger ou de préjudice concret pour les personnes concernées). Le groupe de travail estime que le comité européen de la protection des données devrait en tout état de cause être associé à la définition de ces critères et circonstances.

Pour prendre en compte les recommandations formulées par le groupe de travail et l'ENISA, le formulaire de notification devrait comporter une évaluation de la gravité de la violation des données à caractère personnel, fondée sur des critères objectifs.

En ce qui concerne le rôle et le fonctionnement des autorités chargées de la protection des données

Indépendance

Le texte indique, dans sa version actuelle, que les membres des autorités chargées de la protection des données ne peuvent être nommés que par un parlement ou un gouvernement. Toutefois, le groupe de travail souhaite que les États membres puissent donner la possibilité à d'autres organes indépendants, comme le conseil de la magistrature, de nommer et/ou désigner eux aussi des membres des autorités chargées de la protection des données.

Pouvoirs

Outre la possibilité qui leur est offerte de mener des enquêtes, les autorités chargées de la protection des données devraient également avoir expressément la possibilité de réaliser des audits.

Budget

Pour que les autorités chargées de la protection des données exercent efficacement les fonctions et pouvoirs étendus qui leur incombent au titre du règlement, notamment ceux qu'elles doivent mettre en œuvre dans le cadre de l'assistance mutuelle, de la coopération et de la participation au comité européen de la protection des données, le règlement prévoit que les États membres doivent veiller à ce que lesdites autorités disposent des ressources humaines, techniques et financières appropriées, ainsi que des locaux et de l'infrastructure nécessaires. Comme mentionné plus haut, le groupe de travail recommande vivement d'indiquer de manière plus concrète en quoi consiste un budget adéquat, par exemple après la réalisation d'une évaluation approfondie indépendante des coûts supplémentaires pour les autorités chargées de la protection des données, sur la base des propositions actuelles.

Un budget adéquat pourrait partir d'un montant fixe destiné à couvrir les fonctions de base que toutes les autorités doivent toutes assumer de la même manière, complété par un montant calculé à partir d'une formule tenant compte de la population d'un État membre et de son PIB. Il pourrait également y avoir un élément tenant compte du nombre de multinationales dont le siège est établi dans l'État membre concerné. L'un des considérants devrait expressément encourager les États membres à envisager diverses options de financement de l'autorité chargée de la protection des données, afin de garantir que soit remplie l'obligation d'allouer des ressources suffisantes à l'autorité.

Marge d'appréciation

Les autorités chargées de la protection des données devraient être autorisées à faire des choix pour être efficaces; elles devraient pouvoir définir leurs propres priorités et engager des actions de leur propre initiative, comme des enquêtes, en dépit de leurs obligations en matière de coopération, d'assistance mutuelle et de contrôle de la cohérence conformément au chapitre VII. Les autorités chargées de la protection des données devraient pouvoir allouer des ressources en fonction du caractère stratégique et de la complexité des enjeux, par exemple en tenant compte du préjudice réel ou potentiel pour la protection des données, du nombre de personnes visées et de la technologie utilisée. Le fait d'autoriser ces autorités à fixer leurs propres priorités faciliterait également la gestion des contraintes financières et budgétaires.

Les fonctions prévues à l'article 52, paragraphes 2 et 3, qui indique que les autorités chargées de la protection des données «sensibilise[nt]» et «sur demande, conseille[nt] toute personne concernée», semblent réduire la marge d'appréciation dont ces autorités doivent nécessairement disposer pour être efficaces. En outre, afin que ces autorités bénéficient de cette marge, le groupe de travail suggère d'insérer le verbe «peut» à l'article 34, paragraphe 3, comme suit: «et **peut** formuler des propositions appropriées afin de remédier à cette non-conformité».

Territorialité et compétence des autorités chargées de la protection des données (guichet unique)

L'article 51, paragraphe 1, prévoit qu'une autorité chargée de la protection des données est compétente sur le territoire de l'État membre dont elle relève. Cette règle générale est complétée par l'article 51, paragraphe 2, qui indique que l'autorité chargée de la protection des données d'un État membre où un responsable du traitement a son établissement principal est réputée être l'autorité compétente pour contrôler les activités de traitement dans tous les États membres.

Le groupe de travail est favorable à la création du concept d'autorité chef de file et à l'instauration d'une obligation claire, faite aux autorités chargées de la protection des données, de coopérer et de s'en remettre au mécanisme de contrôle de la cohérence dans les cas où des personnes concernées dans plusieurs autres États membres sont susceptibles d'être affectées par des activités de traitement, car cela permettra une interprétation et une application uniformes du cadre juridique de l'UE, ce qui contribuera à la sécurité juridique. Toutefois, comme mentionné ci-dessus, afin que le mécanisme puisse fonctionner, il convient de clarifier la définition de la notion d'établissement principal et les conséquences sur la compétence des autres autorités chargées de la protection des données. De même, la manière dont est envisagé le mécanisme de contrôle de la cohérence soulève des questions.

En tout état de cause, il doit être clair qu'une autorité chargée de la protection des données qui a été désignée chef de file ne dispose pas d'une compétence exclusive. La compétence de l'autorité chef de file est soumise aux obligations de coopérer, fournir et accepter l'assistance mutuelle et de recourir au mécanisme de contrôle de la cohérence, comme énoncé au chapitre VII sur la coopération et la cohérence, ainsi que d'agir en accord avec les autres autorités chargées de la protection des données concernées.

En outre, le groupe de travail souligne que le principe de guichet unique énoncé à l'article 51, paragraphe 2, ne s'applique que lorsque le responsable du traitement ou le sous-traitant possède plus d'un établissement au sein de l'UE; il ne s'applique pas lorsqu'il n'y a aucun établissement dans l'UE et lorsque les activités de traitement sont liées à l'offre de biens et de services à des personnes concernées dans l'Union ou à l'observation de leur comportement, conformément à l'article 3, paragraphe 2. Par conséquent, dans ce cas, toute autorité chargée de la protection des données dont l'État membre est affecté par des activités de traitement est compétente conformément à l'article 51, paragraphe 1, mais le règlement manque de règles pour déterminer l'autorité «chef de file» dans ces situations. Le groupe de travail estime que la coopération et la cohérence sont tout particulièrement importantes dans ces situations.

Étant donné que les éléments actuellement énoncés pour définir l'établissement principal à l'article 4, paragraphe 13, ne sont pas satisfaisants, comme expliqué plus haut, et qu'il y a donc un manque de clarté quant à la détermination de l'autorité chef de file compétente dans les situations transfrontières, le groupe de travail propose d'envisager:

1. d'accepter que la compétence d'une autorité chef de file est non exclusive, mais subordonnée aux obligations de coopérer, de fournir et d'accepter l'assistance mutuelle et de recourir au mécanisme de contrôle de la cohérence, comme énoncé au chapitre VII sur la coopération et la cohérence; et
2. lorsqu'il n'y a aucun établissement dans l'UE (ou que le lieu de l'établissement principal n'est pas clair), de définir des critères permettant de désigner l'autorité chef de file, qui pourraient être notamment:
    - l'État membre dans lequel les traitements en question ont lieu;
    - l'État membre dans lequel des personnes font l'objet des traitements;
    - l'État membre dans lequel des personnes ont expressément introduit une réclamation ou fait part de leurs préoccupations auprès de l'autorité chargée de la protection des données, conformément à l'article 73, paragraphe 1.

Il est évident qu'il peut y avoir plusieurs États membres pour chacun des critères susmentionnés. Toutefois, à partir de ces critères, les autorités concernées devraient convenir entre elles de celle qui endosse la responsabilité de chef de file. Dans les cas où cette désignation n'est pas évidente ou ne fait pas l'objet d'un accord, le comité européen de la protection des données devrait décider, en se fondant sur les mêmes critères, quelle est l'autorité chef de file.

<u>Assistance mutuelle</u>

Le groupe de travail suggère l'adoption d'un concept global concernant l'autorité chef de file et la coopération. Chaque fois que, au sens de l'article 56, «des personnes concernées dans plusieurs autres États membres sont susceptibles de faire l'objet de traitements», les autorités respectives chargées de la protection des données devraient avoir l'obligation générale de coopérer dans la mesure où leurs citoyens sont affectés. Cette coopération devrait comprendre une appréciation juridique ainsi que l'adoption de mesures de contrôle spécifiques.

Relativement à l'article 55, paragraphe 1, le groupe de travail estime que les autorités chargées de la protection des données devraient se communiquer d'autres informations utiles, également lorsqu'une mesure, au sens de l'article 58, paragraphe 1, n'a pas encore été adoptée (par exemple, en cas de violation de la sécurité). De plus, les autorités chargées de la protection des données devraient se communiquer leurs décisions favorables en ce qui concerne les analyses d'impact relatives à la protection des données.

Le groupe de travail suggère de préciser, aux articles 55 et 56, que chaque fois qu'une décision doit être prise qui implique tant l'autorité chef de file, au sens de l'article 51, paragraphe 2, qu'une autre autorité chargée de la protection des données concernée en vertu de l'article 51, paragraphe 1, l'autorité chef de file et l'autorité nationale «sur place» devraient agir *de concert* en ce qui concerne l'évaluation de la situation et les mesures à adopter. Lorsque les autorités concernées ne parviennent pas à un consensus en ce qui concerne l'évaluation de la situation et/ou les mesures à adopter sur un plan bilatéral ou multilatéral, la situation devrait être soumise au mécanisme de contrôle de la cohérence prévu à l'article 57.

Le groupe de travail salue les mesures proposées pour garantir que les autorités chargées de la protection des données puissent travailler ensemble, et note que la compétence de l'autorité chef de file examinée ci-dessus n'est pas exclusive. Le groupe de travail souligne toutefois qu'il en faut davantage pour assurer l'assistance mutuelle, en termes de budget pour les autorités chargées de la protection des données, comme mentionné ci-dessus, mais également en ce qui concerne la prise en charge de certains détails importants de la mise en pratique de l'assistance mutuelle. La langue utilisée, les délais, la quantité et la nature des informations demandées ainsi que les moyens techniques, les formats et les procédures pour l'échange des informations constituent des questions qui, dans la pratique, sont vitales pour assurer une coopération efficace entre les autorités chargées de la protection des données et sont donc également au cœur du principe de «guichet unique».

Cohérence

Le groupe de travail se félicite que sa proposition relative à un mécanisme de coopération et de coordination destiné à garantir une application cohérente des règles en matière de protection des données ait été introduite aux articles 57 et 58 de la proposition.

Le groupe de travail estime toutefois que ce mécanisme devrait assurer une cohérence uniquement dans les domaines où cela est nécessaire, qu'il ne devrait pas empiéter sur l'indépendance des autorités de contrôle nationales et les différents acteurs devraient conserver leurs responsabilités telles qu'elles sont réparties.

Au vu de la large portée de l'article 58, paragraphe 2, point a), qui couvre le traitement de données dans le cadre de tout type d'offre transfrontière de biens ou services au sein de l'UE, le groupe de travail suggère que ne soient soumis au comité européen de la protection des données, dans le cadre du mécanisme de contrôle de la cohérence, que les cas dans lesquels les autorités compétentes, conformément à l'article 51, ne parviennent pas à un consensus sur l'évaluation de la situation et/ou les mesures à adopter sur un plan bilatéral ou multilatéral. En tout état de cause, le comité européen de la protection des données devrait être informé des situations présentant un intérêt général pour la protection des données ou la libre circulation des données à caractère personnel au sein de l'UE.

Afin d'éviter qu'un grand nombre de dossiers ne soient ouverts en raison de la portée très large du mécanisme (du fait de l'article 58, paragraphe 3, qui indique que **toute** autorité peut demander que toute question soit traitée dans le cadre du mécanisme de contrôle de la cohérence), le groupe de travail suggère de soumettre à un vote au sein du comité européen de la protection des données les demandes présentées au titre de l'article 58, paragraphe 3.

En dépit du rôle de gardienne des traités de la Commission, le groupe de travail émet de sérieuses réserves quant au rôle envisagé pour la Commission en ce qui concerne les cas particuliers en cours d'examen dans le cadre du mécanisme de contrôle de la cohérence,

puisqu'il empiète sur l'indépendance des autorités chargées de la protection des données et du comité européen de la protection des données. Lorsqu'une question est examinée ou a été examinée par le comité européen de la protection des données dans le cadre de ce mécanisme, la Commission devrait être en mesure de donner son appréciation juridique tout en s'abstenant en principe d'intervenir. Cela vaut particulièrement en cas de suspension d'une mesure, comme énoncé à l'article 60, paragraphe 1, et à l'article 62, paragraphe 1, point a), et paragraphe 2. De plus, l'existence de «doutes sérieux» n'est pas suffisante pour déclencher l'intervention de la Commission.

Le groupe de travail souligne qu'il appartient au comité européen de la protection des données de veiller à ce que ses avis soient respectés et appliqués de manière uniforme par toutes les autorités concernées chargées de la protection des données.

Afin d'accroître l'efficacité des avis du comité européen de la protection des données, un «mécanisme de confirmation» pourrait être introduit pour le cas où une ou plusieurs autorités chargées de la protection des données entendent déroger à un avis adopté par le comité dans le cadre du mécanisme de contrôle de la cohérence, conformément à l'article 58, paragraphe 7. Le comité devrait, dans ce cas, être en mesure de reconfirmer son avis par un vote à la majorité qualifiée, soulignant ainsi l'importance d'une approche commune pour les situations présentant un intérêt général pour la protection des données au sein de l'UE. Une autre solution consisterait à offrir aux autorités chargées de la protection des données la possibilité d'exprimer des positions minoritaires. Ces positions devraient être motivées et rendues publiques.

De plus, il conviendrait d'envisager une procédure pour permettre au comité européen de la protection des données et à la Commission de solliciter l'avis de la Cour de justice de l'Union européenne sur l'interprétation du règlement, au cas où une autorité chargée de la protection des données aurait l'intention de ne pas suivre un avis reconfirmé par le comité européen à l'issue d'un vote à la majorité qualifiée.

Application de la législation nationale (chapitre IX)

Lorsque des règles particulières seront adoptées dans les États membres au titre des articles 80 à 83, ces règles s'articuleront avec les règles relatives à la compétence des autorités chargées de la protection des données et au mécanisme d'autorité chef de file.

Le texte ne résout pas, dans sa version actuelle, la question des cas découlant de la législation nationale connexe, par exemple dans le contexte du travail, par rapport au champ de compétence de l'autorité chargée de la protection des données dont relève l'établissement principal du responsable du traitement. La question est de savoir si, par exemple, l'autorité allemande chargée de la protection des données serait tenue d'interpréter et d'appliquer la législation du travail espagnole en cas de litige concernant un salarié d'une filiale espagnole d'une société dont l'établissement principal se situe en Allemagne. Il faudrait dès lors préciser que, par dérogation à l'article 51, paragraphe 2, pour les cas subordonnés à l'application de la législation nationale conformément au chapitre IX du règlement, l'autorité nationale chargée de la protection des données devrait toujours (en coopérant, bien entendu, avec l'autorité chef de file) être compétente pour appliquer la législation nationale connexe dans ce cas particulier (dans l'exemple donné ci-dessus, l'autorité espagnole chargée de la protection des données serait compétente pour appliquer, dans le contexte du travail, la législation espagnole en matière de protection des données).

D’une manière générale, le groupe de travail souligne la nécessité de clarifier le champ d’application des lois nationales adoptées au titre du chapitre IX.

Délais

Le groupe de travail convient qu’il est important que les avis du comité européen de la protection des données sollicités par le biais du mécanisme de contrôle de la cohérence soient émis en temps utile. Le délai imparti pour obtenir des résultats devrait toutefois permettre d'assurer la qualité des conseils. Afin de garantir une influence et un soutien effectifs sur le terrain et de garantir que l’avis puisse être confirmé dans le cadre d’une éventuelle procédure juridictionnelle, le délai strict qui est proposé devra en tout état de cause être étendu.

<u>«Guichet unique» pour les personnes concernées</u>

À l’instar des responsables du traitement, les personnes concernées relevant de la compétence des autorités chargées de la protection des données dans les pays de l’UE devraient également disposer d’un «guichet unique». Dans le règlement, plusieurs possibilités sont offertes aux personnes concernées pour exercer leurs droits et demander justice. Les personnes concernées peuvent introduire une réclamation auprès d’une autorité chargée de la protection des données dans tous les États membres (auprès de leur autorité nationale chargée de la protection des données, de l’autorité de l’État membre où le responsable du traitement a son établissement principal ou auprès de toute autre autorité de l’Union). Les personnes concernées peuvent également engager une action devant leur juridiction nationale et devant la juridiction du pays où le responsable du traitement a un établissement.

Si ces possibilités peuvent vraisemblablement accroître les droits des personnes concernées, elles peuvent également entraîner de la confusion et de l’incertitude quant à l’entité qui sera chargée, en définitive, de fournir une réponse à la personne concernée.

En dépit du droit d’introduire un recours juridictionnel, le groupe de travail suggère de préciser que les personnes concernées doivent, en principe, contacter l’autorité chargée de la protection des données du pays où elles résident ou celle du pays où le responsable du traitement ou le sous-traitant a un établissement. Afin de pouvoir répondre à la personne concernée, l’autorité sollicitée dans cet État membre serait tenue de coopérer avec l’autorité dont relève l’établissement principal du responsable du traitement (l’autorité chef de file) afin de convenir des mesures nécessaires pour procéder à l’examen du dossier et, dans certains cas, pour faire respecter le règlement. Toutefois, dans toutes les circonstances, c’est l’autorité initialement sollicitée qui restera chargée de répondre à la personne concernée.

<u>Structure institutionnelle du comité européen de la protection des données</u>

Le groupe de travail note qu’il sera remplacé par le comité européen de la protection des données, institué à l’article 64.

Le groupe de travail estime qu’il devrait pouvoir choisir de manière démocratique ses propres président et vice-présidents. Il estime qu'aucune raison convaincante n’a été avancée pour exiger que le contrôleur européen de la protection des données (CEPD) en soit un vice-président permanent.

En outre, il serait souhaitable de disposer d'un secrétariat entièrement indépendant. Or, le groupe de travail relève que le secrétariat du comité doit être assuré par le CEPD et non plus par la Commission. Il conviendrait de réfléchir plus avant à cette organisation en termes de dispositions pratiques et de rapports hiérarchiques, en particulier en ce qui concerne la nécessité de garantir l'indépendance des membres du secrétariat et les conséquences juridiques et institutionnelles liées au fait de confier le secrétariat du comité à l'un de ses membres.

Transferts internationaux

Le règlement souligne à juste titre la responsabilité qui incombe aux responsables du traitement de garantir que les données à caractère personnel demeurent protégées lorsqu'elles sont transférées en dehors de l'espace économique européen (EEE). Il simplifie la tâche des responsables du traitement en prévoyant diverses «sphères de sécurité» sous la forme de décisions relatives au caractère adéquat du niveau de protection, d'un système rationalisé de règles d'entreprise contraignantes pour les multinationales, de clauses contractuelles approuvées et d'une autorisation par l'autorité chargée de la protection des données. Il prévoit également diverses dérogations à l'article 44.

Toutefois, les dérogations, en particulier à l'article 44, paragraphe 1, point h), demeurent très étendues et pourraient s'appliquer à de nombreuses situations. Conformément à l'avis précédent du groupe de travail (WP 114), ces dérogations ne devraient être applicables que dans la mesure où le traitement n'est pas massif, pas répétitif et pas structurel.

De plus, l'article 42 introduit la possibilité de recourir à des instruments non contraignants pour encadrer les transferts internationaux, qui sont soumis à l'autorisation des autorités chargées de la protection des données. Or, le caractère contraignant a toujours été considéré comme une exigence importante dans les outils qui encadrent actuellement les transferts internationaux (par exemple, clauses contractuelles types, règles d'entreprise contraignantes, sphère de sécurité, niveau de protection adéquat assuré dans les pays tiers). Dès lors, le groupe de travail propose de supprimer l'article 42, paragraphe 5, à l'exception de la dernière phrase. Le renvoi figurant à l'article 34 doit donc être adapté en conséquence.

Concernant l'article 41, paragraphe 6, il conviendrait de préciser si les termes «sans préjudice des articles 42 à 44» signifient qu'en cas de décision négative relative au caractère adéquat du niveau de protection prise par la Commission, les transferts de données vers le pays tiers concerné sont néanmoins possibles en vertu de l'ensemble de ces articles.
Pour finir, lorsque la Commission constatera par voie de décision qu'un pays tiers, ou un territoire ou un secteur de traitement de données dans ce pays tiers ou l'organisation internationale en question assure un niveau de protection adéquat (article 41), ledit transfert ne nécessitera aucune autre autorisation. Toutefois, comme mentionné auparavant, le groupe de travail suggère vivement d'inclure l'obligation pour la Commission de consulter le comité européen de la protection des données au sujet des décisions relatives au caractère adéquat du niveau de protection.

Divulgations non autorisées par la législation de l'UE

Le groupe de travail souligne la nécessité d'inclure dans le règlement le recours obligatoire aux traités d'entraide judiciaire en cas de divulgations non autorisées par la législation de

l'Union ou des États membres. Il estime que l'absence de disposition sur le recours obligatoire aux traités d'entraide judiciaire, lorsqu'ils existent, laisserait notamment la voie ouverte à de larges transferts de données à caractère personnel pour une catégorie vaste et illimitée de «motifs importants d'intérêt général», conformément à l'article 44, paragraphe 1, point d), y compris lorsque ces transferts revêtent un caractère massif, fréquent et structurel. Lorsque le jugement d'une cour ou d'un tribunal ou la décision d'une autorité administrative d'un pays tiers exige d'un responsable du traitement ou d'un sous-traitant qu'il transfère des données de l'UE vers ce pays tiers et qu'il n'existe aucun traité d'entraide judiciaire ou autre accord international en vigueur entre le pays tiers demandeur et l'Union ou le ou les États membres, le transfert desdites données devrait être interdit. Le groupe de travail souligne que lorsqu'un traité d'entraide judiciaire est en vigueur, l'autorité compétente au titre dudit traité (ou d'un accord international analogue) devrait être l'autorité traitant la demande, laquelle devrait, si nécessaire, consulter l'autorité chargée de la protection des données.

Droit à réparation et responsabilité

Le groupe de travail salue la disposition introduite à l'article 77, paragraphe 1, pour garantir que toute personne ayant subi un dommage du fait d'un traitement illicite ou de toute action incompatible avec le règlement a le droit d'obtenir du responsable du traitement ou du sous-traitant réparation du préjudice subi. Il salue également le fait que l'article 77, paragraphe 2, garantisse que, lorsque plusieurs responsables du traitement ou sous-traitants ont participé au traitement, il n'incombe pas à la personne concernée de déterminer lequel d'entre eux porte la responsabilité du préjudice. Il estime toutefois qu'il est nécessaire de préciser (dans un considérant) que le terme «préjudice» ou «dommage» ne signifie pas simplement un préjudice matériel mais également une souffrance (un préjudice qui n'est pas matériel).

Si une décision prise par une autre autorité chargée de la protection des données (par exemple, l'autorité dont relève l'établissement principal) affecte la personne concernée ou lui cause un préjudice, cette dernière devrait être en mesure d'intenter une action contre cette décision devant les juridictions administratives de son pays de résidence.

La solution telle qu'elle est proposée par la Commission européenne, à savoir que soit la personne concernée soit l'autorité chargée de la protection des données puisse intenter une action contre l'autre autorité sur le territoire de cette dernière, est loin d'être satisfaisante. Le groupe de travail demande qu'un système permette aux personnes concernées d'intenter une action contre une décision administrative devant la juridiction administrative de leur pays de résidence.

Amendes

Le groupe de travail salue l'instauration d'amendes importantes, parce que celles-ci permettront aux autorités chargées de la protection des données d'assumer leur rôle d'autorité répressive et qu'elles pourront, par leur effet dissuasif, contribuer à un plus grand respect de l'instrument de la part des responsables du traitement.

L'article 79, paragraphe 1, prévoit que chaque autorité de contrôle soit «habilitée» à infliger des sanctions administratives. Le considérant 120 soutient cette disposition en indiquant que l'autorité de contrôle «devrait avoir le pouvoir» de sanctionner les infractions administratives. Toutefois, les paragraphes 4 à 6 de l'article 79 indiquent que l'autorité de contrôle «inflige une amende» dans les situations décrites. Le groupe de travail est d'avis que les autorités

chargées de la protection des données devraient disposer d'une marge d'appréciation pour décider des situations dans lesquelles elles infligent une amende, puisque de nombreux facteurs influent sur la nature de l'infraction et doivent être pris en compte lorsqu'il est décidé d'infliger une amende. Il suggère dès lors de modifier en conséquence le libellé de l'article 79, paragraphes 4 à 6.

Le groupe de travail apprécie l'effet d'harmonisation produit par l'article 79, qui détermine à quelle amende maximum une infraction donne lieu, puisque cela permettra une plus grande cohérence des amendes infligées dans l'Union européenne. Néanmoins, il suggère d'expliciter à l'article 58, paragraphe 2, la possibilité de recourir au mécanisme de contrôle de la cohérence, prévu à la section 2 du chapitre VII, pour résoudre les divergences d'application des sanctions administratives, comme le prévoit également le considérant 120.

Par ailleurs, le groupe de travail comprend que lorsque plusieurs autorités chargées de la protection des données sont compétentes, elles sont toutes habilitées à infliger une amende en vertu de l'article 79 du règlement. Cela soulève cependant des questions quant au principe non bis in idem (interdiction de la double incrimination).

En outre, le groupe de travail pense que du fait du seuil introduit en cas de premier manquement non intentionnel au règlement, de nombreux responsables du traitement échapperaient, dans la pratique, à son application, et il estime donc que ce seuil devrait être supprimé. Si un seuil devait être introduit, il serait en tout état de cause plus approprié de tenir compte du nombre de personnes concernées affectées (de manière négative) que du nombre de salariés du responsable du traitement.

Recours juridictionnels

Le groupe de travail salue l'inclusion d'un ensemble de règles complet sur les recours juridictionnels ouverts aux personnes concernées, y compris la possibilité pour les organisations ou associations d'exercer les droits des personnes concernées vis-à-vis des responsables du traitement et des sous-traitants. Toutefois, de l'avis du groupe de travail, plusieurs aspects du chapitre VIII exigent un éclaircissement.

Vu l'étendue du champ d'application de l'article 73, paragraphe 1, en vertu duquel toute personne concernée a le droit d'introduire une réclamation auprès d'une autorité chargée de la protection des données dans **tout** État membre, le groupe de travail estime que la personne concernée devrait, en principe, saisir l'autorité chargée de la protection des données de son pays de résidence ou du pays où est établi le responsable du traitement ou le sous-traitant, comme le groupe de travail l'a également indiqué ci-dessus à propos du guichet unique pour les personnes concernées.

En outre, lorsque l'autorité chargée de la protection des données qui reçoit la réclamation semble ne pas être la bonne au vu du fond de l'affaire, le groupe de travail estime que cette autorité devrait avoir l'obligation de coopérer avec l'autorité «guichet unique» de la personne concernée et l'autorité du lieu où est établi le responsable du traitement. Dans ce cas, l'autorité chargée de la protection des données auprès de laquelle la réclamation a été introduite serait tenue d'informer la personne concernée de l'évolution de l'affaire, indépendamment du fait qu'elle soit compétente ou non quant au fond de l'affaire. Il s'agit d'un corollaire de la nécessité de désigner un guichet unique pour les personnes concernées (voir ci-dessus).

En ce qui concerne l'article 74, paragraphe 2, le groupe de travail estime qu'il conviendrait de préciser quelle autorité chargée de la protection des données est compétente pour «donner suite à une réclamation, en l'absence d'une décision nécessaire pour protéger [les] droits [de la personne concernée]». Lorsqu'une autorité chef de file serait visée par un recours, l'autorité compétente pour donner suite à la réclamation serait, conformément à l'article 51, paragraphe 2, celle de l'État membre où le sous-traitant/responsable du traitement a son établissement principal, et dans tout autre cas il s'agirait de l'autorité compétente conformément à l'article 51, paragraphe 1. Il conviendrait donc de préciser à l'article 74, paragraphe 2, que l'obligation de donner suite renvoie à l'autorité de contrôle compétente «[...] au sens de l'article 51, paragraphe 1 ou paragraphe 2».

De plus, l'article 74, paragraphe 4, dispose qu'une personne concernée affectée par une décision prise par l'autorité chargée de la protection des données d'un État membre autre que celui dans lequel ladite personne a sa résidence habituelle peut demander à l'autorité de l'État membre dans lequel elle a sa résidence habituelle d'intenter une action contre l'autorité de l'autre État membre. Si le groupe de travail comprend ce qui motive l'introduction d'une disposition de ce type, qui veille à ce que les personnes concernées puissent exercer leurs droits vis-à-vis d'une autorité chargée de la protection des données dans un autre État membre, il considère néanmoins qu'elle est contraire à l'obligation générale faite aux autorités chargées de la protection des données de coopérer et de se prêter mutuellement assistance dans les affaires transfrontières, conformément aux articles 55 et 56, et au fait qu'en cas de désaccord entre lesdites autorités, le comité européen de la protection des données doit être saisi de l'affaire. Dès lors, le groupe de travail souligne la nécessité d'examiner attentivement d'autres possibilités de recours juridictionnel pour la personne concernée à l'encontre d'une décision prise par une autorité à son détriment, qui soient cohérentes avec les principes du règlement.

L'article 75, paragraphe 2, prévoit la possibilité pour les personnes concernées d'intenter une action contre un responsable du traitement ou un sous-traitant devant les juridictions de l'État membre dans lequel le responsable du traitement ou le sous-traitant dispose d'un établissement, ou d'intenter une telle action devant les juridictions de l'État membre dans lequel la personne concernée a sa résidence habituelle. Le groupe de travail estime que la possibilité d'intenter une action devant les juridictions de **tout** État membre dans lequel le responsable du traitement ou le sous-traitant a un établissement, indépendamment du fait qu'il s'agisse de l'établissement principal ou de l'établissement dans lequel les décisions pertinentes en matière de traitement des données sont prises, peut poser problème.

Bien que l'article 75, paragraphe 4, indique que les États membres doivent mettre à exécution les décisions définitives rendues par les juridictions des autres États membres, il n'est pas certain qu'une décision prise par une juridiction dans un État membre où le responsable du traitement ou le sous-traitant n'a pas son établissement principal soit réellement exécutoire. Ce point exige une clarification.

En outre, même si le groupe de travail salue le fait qu'ait été incluse à l'article 75, paragraphe 2, la possibilité d'intenter une action contre un responsable du traitement devant les juridictions de l'État membre dans lequel la personne concernée a sa résidence habituelle - par analogie avec la notion de protection du consommateur conformément au règlement Bruxelles I -, dans le but de renforcer la position des personnes concernées, on ne voit pas clairement comment serait exécuté le jugement d'une juridiction de l'État membre dans lequel

la personne concernée a sa résidence habituelle si le responsable du traitement ou le sous-traitant est établi dans un autre État membre.

Tant l'article 74, paragraphe 5, que l'article 75, paragraphe 4, prévoient que les États membres mettent à exécution les décisions définitives des juridictions visées dans ces articles. Ces dispositions sont comparables à des obligations similaires énoncées à l'article 111 de la convention d'application de l'accord de Schengen. Comme indiqué ci-dessus, on ne sait pas exactement en vertu de quelles règles de procédure et par quelles autorités nationales les décisions rendues par les juridictions d'un État membre seraient exécutées dans un autre État membre. En outre, en ce qui concerne la détermination de ce qui constitue une décision «définitive», une harmonisation plus poussée pourrait se révéler indispensable (Système d'information Schengen – affaire AU/FR).

Églises et associations religieuses

Le groupe de travail comprend que l'article 85 oblige les églises et les associations religieuses qui ont à l'heure actuelle des régimes juridiques distincts à les mettre en conformité avec le règlement. Cela ne confère aucunement aux églises et aux associations religieuses la possibilité d'adopter, dans les États membres où les dispositions constitutionnelles ne permettent pas une telle mise en conformité, un régime juridique distinct qui serait incompatible avec le règlement.

En ce qui concerne la directive

Choix de l'instrument

Le groupe de travail prend note du choix explicite fait par la Commission européenne de ne pas présenter un instrument unique pour la protection des données dans tous les domaines, et de présenter une directive pour être l'instrument réglementant la protection des données dans le domaine de la police et de la justice pénale, au niveau élevé et constant visé par la Commission en la matière. Toutefois, le groupe de travail note également que la proposition actuelle entraînerait un abaissement des normes en matière de protection des données dans plusieurs États membres. Cette perspective est pour lui inacceptable et il prie donc le législateur européen de veiller à ce que les garanties les plus élevées en matière de protection des données en vigueur dans l'Union européenne soient considérées comme le strict minimum pour la proposition de directive. La directive ne devrait pas être interprétée de manière à justifier la suppression de garanties supplémentaires en matière de protection des données prévues par la législation actuelle de certains États membres.

Cohérence

Bien que différents instruments soient proposés, les aspects «fondamentaux» des dispositions doivent être cohérents, en particulier en ce qui concerne les principes, obligations et responsabilités, droits et pouvoirs, et les outils mis à la disposition des autorités de contrôle. En effet, compte tenu du caractère sensible des traitements qui font l'objet de la directive, il serait inacceptable que des normes moins élevées s'appliquent à ce domaine. Bien entendu, il est nécessaire de prévoir des limitations et des exceptions, notamment en ce qui concerne les

droits des personnes concernées, mais il doit être clair qu'il s'agit d'exceptions et que les aspects «fondamentaux» demeurent les mêmes.

Champ d'application

Le groupe de travail note et salue le fait que la directive ait abandonné la distinction entre le traitement de données à caractère personnel dans les affaires nationales et celui dans les affaires transfrontières, qui était prévue dans la décision-cadre 2008/977/JAI. Cette limitation de l'applicabilité de la législation européenne aux affaires strictement transfrontières a été critiquée par le groupe de travail dans le passé.

Le champ d'application de la directive doit être aussi clair que possible. Toutefois, le texte proposé soulève diverses questions, dont les suivantes.

Le groupe de travail note la difficulté qu'il y a à distinguer le champ d'application de la directive du champ d'application du règlement. La directive s'applique si les autorités compétentes traitent des données à caractère personnel à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales. Dans toutes les autres circonstances, c'est le règlement qui s'applique, en tant qu'instrument général de protection des données à caractère personnel. Toutefois, il y a lieu de tenir compte des différentes pratiques des États membres lorsqu'ils définissent les activités de leurs autorités qui se rattachent à des fins répressives ou simplement administratives (par exemple, dans les domaines des douanes, de l'immigration, de l'environnement). Par conséquent, les deux instruments, la directive et le règlement, seraient susceptibles de s'appliquer à une même institution. Il faut éviter les situations dans lesquelles une même opération de traitement, par exemple en lien avec le maintien de l'ordre public, serait, dans un pays, couverte par le règlement, tandis que dans d'autres États membres ce seraient les lois basées sur la directive qui s'appliqueraient. Cela pose particulièrement problème si les deux instruments manquent de cohérence, comme c'est le cas actuellement. De ce point de vue, il faut davantage de cohérence entre les deux instruments et une plus grande clarté serait nécessaire en ce qui concerne la définition des «autorités compétentes». Le groupe de travail estime qu'il faut définir clairement quelles sont les missions, dont les autorités compétentes sont investies par la loi, auxquelles s'applique la directive.

Le groupe de travail est d'avis qu'il faut préciser davantage dans quelle mesure la directive s'applique au domaine de la procédure pénale. Il note que la directive s'applique au traitement des données aux fins de la poursuite des infractions pénales (article premier). Dans le même temps, le groupe de travail comprend qu'il faut entendre par l'article 17 (et le considérant 82) que les États membres peuvent décider de ne pas aligner leurs règles nationales en matière de procédure pénale sur les droits prévus aux articles 11 à 16, du moins dans les cas qui concernent les procédures judiciaires. Les différences qui existent en matière de procédure pénale nationale, toutefois, ne permettent pas de déterminer facilement de quelle phase des poursuites il est question lorsque la directive, à l'article 17, indique que, «lorsque les données à caractère personnel figurent dans une décision judiciaire ou un casier judiciaire faisant l'objet d'un traitement lors d'une enquête judiciaire ou d'une procédure pénale, les droits […] sont exercés conformément aux règles nationales de procédure pénale». Le groupe de travail invite le législateur européen à s'assurer qu'il ne puisse subsister aucun doute quant au fait que la directive s'applique aux procédures pénales et à la poursuite d'infractions pénales, également pour éviter les cas dans lesquels une protection des données ne serait pas assurée

dès qu'un procureur ou un juge d'instruction participe à une opération répressive ou à une enquête, conformément à la convention 108 du Conseil de l'Europe.
En outre, le groupe de travail estime que l'article 44, paragraphe 2, requiert une clarification quant au sens et à l'intention à prêter aux termes «dans l'exercice de leurs fonctions juridictionnelles». Il convient de préciser quelle doit être la relation entre l'autorité chargée de la protection des données et les juridictions et dans quelles circonstances des missions de contrôle peuvent être effectuées.

Principes de traitement des données

En ce qui concerne les principes, la directive n'intègre pas d'éléments importants relatifs à la conservation des données à caractère personnel (notamment des durées de conservation), à la transparence envers les personnes physiques, à la mise à jour des données à caractère personnel et à la vérification du caractère adéquat, pertinent et non excessif des données conservées. Il manque également des dispositions en matière de responsabilité qui exigeraient du responsable du traitement qu'il prouve son respect de l'instrument. Le libellé de l'article 4 devrait être rendu concordant avec le libellé figurant dans le règlement (article 5).

Le groupe de travail suggère en outre d'inclure des dispositions limitant l'accès aux données au personnel dûment autorisé des autorités compétentes qui en a besoin pour l'exécution de ses missions.

Outre les observations formulées ci-dessus concernant le manque de cohérence avec le règlement, le groupe de travail salue la distinction proposée entre les différentes catégories de personnes concernées devant faire l'objet d'un traitement. Il note en particulier la distinction devant être faite entre les données relatives à des suspects, des victimes, des témoins, etc. De même, il salue la distinction devant être faite en fonction de la qualité et la précision des données traitées par les services répressifs. Le groupe de travail regrette toutefois que ces distinctions soient limitées par l'ajout des termes «dans la mesure du possible» aux articles 5 et 6, termes qu'il propose de supprimer. Par ailleurs, il s'inquiète de l'ampleur de la catégorie de personnes concernées classées «divers» [article 5, paragraphe 1, point e)] dont les données peuvent faire l'objet d'un traitement. Le groupe de travail suggère de reformuler cette catégorie pour veiller à ce que les données de personnes non soupçonnées ne puissent être traitées que pendant une durée limitée et dans des conditions strictes. La directive devrait préciser que des règles plus strictes doivent s'appliquer en termes de délais et de contrôle aux catégories de personnes concernées mentionnées à l'article 5, paragraphe 1, points b) à e).

En ce qui concerne la licéité du traitement (article 7), la raison de l'insertion des dispositions des points b), c) et d) n'est pas claire. Ces dispositions semblent en contradiction avec l'article premier, paragraphe 1, qui définit l'objet de la directive. Le groupe de travail considère qu'on ne saurait autoriser des traitements qui ne sont pas conformes à l'objet général de la directive. Ainsi, il faut soit supprimer les dispositions des points b), c) et d), soit adapter l'article premier, paragraphe 1, afin de permettre ces traitements.

Le groupe de travail estime que des dispositions particulières devraient être introduites à propos du traitement des données à caractère personnel concernant des enfants, comme le prévoit le règlement. En particulier, il faudrait obliger les États membres à prévoir des seuils d'âge en deçà desquels les données ne devraient pas être traitées à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière sans que cela ne soit dûment justifié, en particulier si des catégories particulières de données doivent être

collectées. De plus, il faudrait que les États membres prévoient pour les données concernant les enfants des durées de conservation plus courtes dans les fichiers de la police et de la justice.

La disposition sur les catégories particulières (article 8) est légèrement plus étendue que dans la décision-cadre 2008/977/JAI. Le groupe de travail s'interroge sur les conséquences que cela peut avoir, et se demande notamment si les dérogations énoncées au paragraphe 2 pourraient donner lieu, dans la législation nationale, à une clause générale indiquant que toutes les données sensibles peuvent être traitées. Dans ce cas, l'interdiction générale ne sert à rien. De plus, bien que les données génétiques soient mentionnées, aucun considérant distinct ni article ne traite du traitement de ce type de données. Une telle disposition constituerait pourtant une garantie importante par ce qui est de l'utilisation des données génétiques et de leurs durées de conservation.

Compte tenu de la dérogation énoncée à l'article 8, paragraphe 2, il existe un danger réel que des niveaux différents de protection des données à caractère personnel (données sensibles) soient autorisés au titre de la directive. Le groupe de travail suggère dès lors que le législateur européen modifie cet article par une définition plus précise des garanties appropriées exigées, afin de permettre une application harmonisée. De plus, le groupe de travail recommande d'ajouter au paragraphe 2 qu'il ne peut être recouru aux exceptions que dans le respect des conditions énoncées à l'article 4.

Droits des personnes concernées

Le groupe de travail note et salue le fait qu'en vertu de l'article 11, paragraphe 1, et de l'article 13, paragraphe 1, davantage d'informations pourraient être communiquées aux personnes concernées, du moins dans certains États membres. Être informé de la nature des données traitées et du motif de leur traitement est l'un des aspects clés du droit à la protection des données. Toutefois, il y a lieu de relever, également, que les limitations apportées à l'obligation d'informer la personne concernée et au droit d'accès, prévues à l'article 11, paragraphe 5, et à l'article 13, paragraphe 2, posent problème. Le groupe de travail considère ces limitations et dérogations comme étant trop vastes et de nature trop générale, puisqu'elles permettent aux États membres de soustraire des catégories entières de données de l'obligation de fournir des informations. Les droits des personnes concernées (et pas seulement leurs intérêts, comme indiqué au chapitre II) s'en trouveraient considérablement limités. La directive devrait donc préciser que toute limitation des droits des personnes concernées ne peut être justifiée qu'au cas par cas, en tenant dûment compte des circonstances du cas particulier et du fait que chacune de ces restrictions (et pas seulement les omissions) doit être pleinement justifiée. En outre, le groupe de travail estime qu'une limitation du droit d'accès et d'information devrait également signifier que, dans certains cas, les personnes concernées peuvent tout de même être partiellement informées du traitement de leurs données.

En ce qui concerne les limitations apportées aux droits, il y a lieu de préciser que le responsable du traitement devrait apprécier au cas par cas si la limitation des droits doit être appliquée, et que toute limitation doit être conforme à la charte des droits fondamentaux de l'Union européenne et à la convention de sauvegarde des droits de l'homme et des libertés fondamentales, et en accord avec la jurisprudence de la Cour de justice de l'Union européenne et de la Cour européenne des droits de l'homme, et en particulier respecter le contenu

essentiel de ces droits et libertés. Le groupe de travail recommande d'insérer ce libellé à l'article 13.

La directive semble être cohérente avec le règlement en ce qui concerne le droit à rectification, le droit d'introduire une réclamation, le droit de recours contre l'autorité nationale chargée de la protection des données, le responsable du traitement et le sous-traitant, et le droit à réparation et la responsabilité.

Toutefois, la directive ne prévoit aucun droit d'opposition au traitement des données à caractère personnel. Il existe de nombreuses situations dans lesquelles, par exemple, des personnes concernées, victimes ou témoins devraient pouvoir faire procéder au marquage de leurs données pour limiter tout traitement ultérieur à l'issue de l'action en justice.

De même, dans la directive les responsables du traitement sont priés de répondre «sans retard indu» aux demandes des personnes physiques exerçant leurs droit d'accès, droit à rectification et droit à l'effacement. On ne voit pas clairement pourquoi les délais imposés dans le règlement ne peuvent pas également s'appliquer en l'espèce. De plus, les modalités selon lesquelles les personnes physiques peuvent exercer leurs droits devraient être davantage alignées sur les procédures décrites dans le règlement.

Obligations des responsables du traitement

Les obligations qui incombent aux responsables du traitement sont cohérentes avec celles prévues dans le règlement en ce qui concerne les sous-traitants, les accords avec les responsables conjoints du traitement, la coopération obligatoire avec l'autorité nationale chargée de la protection des données et les missions du délégué à la protection des données. Toutefois, au titre de la directive, le responsable du traitement n'est pas tenu d'informer la personne physique s'il prévoit de transférer des données à caractère personnel vers un pays tiers, et on ne voit pas clairement ce qui a motivé d'exclure cette obligation, en particulier au vu du fait que les États membres ont la possibilité de restreindre les droits des personnes physiques dans certaines circonstances.

De plus, le libellé de la directive n'est pas cohérent avec le règlement en ce qui concerne la protection des données dès la conception et la protection des données par défaut, le groupe de travail ne pouvant expliquer ce manque de cohérence. L'un des aspects de la prise en compte du respect de la vie privée dès la conception consiste à déterminer les risques du traitement au début du processus pour pouvoir les atténuer. Dès lors, le groupe de travail conseille vivement d'insérer dans la directive des dispositions exigeant une analyse d'impact relative à la protection des données, y compris pendant la procédure législative. Il estime que ces dispositions sont particulièrement importantes dans le domaine du traitement de données à caractère personnel en matière répressive, compte tenu des risques accrus que représente ce traitement pour les personnes physiques. Les obligations relatives à la documentation sont également moins détaillées que dans le règlement. Il faudrait que les autorités compétentes concernées par la directive soient au moins tenues de consigner les coordonnées de leur délégué à la protection des données et les durées de conservation.

Le groupe de travail relève que les exigences relatives à la sécurité des données ne sont pas très détaillées et donc plutôt faibles par rapport aux normes actuelles. À titre d'exemple, les dispositions sur les obligations en matière de sécurité ne comprennent aucune protection contre les pertes ou dommages accidentels, comme le prévoit le règlement. Le groupe de

travail demande instamment au législateur européen d'inclure cet élément dans la directive, en particulier parce que cet aspect figure tant dans la directive actuelle (95/46/CE) que dans la décision-cadre sur la protection des données (2008/977/JAI).

Les dispositions sur la notification des violations devraient également être cohérentes d'un instrument à l'autre, le groupe de travail admettant toutefois les différences qui existent dans le secteur répressif en ce qui concerne la notification des personnes physiques. Par exemple, il peut arriver qu'il ne soit pas possible d'informer des personnes physiques d'une violation dans les délais spécifiés, ceci pouvant porter préjudice à des enquêtes ou opérations menées par les services répressifs. L'autorité chargée de la protection des données peut également jouer un rôle particulier dans l'appréciation de la nécessité d'informer la personne physique et du moment opportun pour le faire, en tenant également compte du caractère approprié des mesures prises en termes de protection technologique.
Pour finir, les dispositions sur le profilage et le traitement automatisé (article 9) ne sont pas cohérentes avec le règlement, en ce que le libellé de la directive n'intègre pas certains éléments pertinents, comme l'évaluation du comportement.

Transferts internationaux

Principes généraux applicables aux transferts et aux transferts ultérieurs

L'article 33 contient des dispositions relatives aux transferts initiaux et aux transferts ultérieurs de données à caractère personnel vers des pays tiers ou des organisations internationales. Le groupe de travail estime qu'il faut clairement distinguer ces situations et prévoir davantage de restrictions pour les transferts ultérieurs, par exemple l'existence d'un lien évident avec la finalité pour laquelle les données ont initialement été collectées et l'obtention du consentement préalable de l'autorité émettrice. En outre, le destinataire des données doit être une autorité compétente au sens de la directive.

Décisions négatives relatives au caractère adéquat du niveau de protection

Le groupe de travail ne voit pas clairement quelle serait la finalité des décisions négatives relatives au caractère adéquat du niveau de protection et comment elles fonctionneraient dans la pratique. Le libellé laisse entendre qu'une décision négative bloquerait tous les transferts internationaux vers le pays tiers, l'organisation internationale ou le secteur de traitement de données en question. L'article 34, paragraphe 6, et l'article 35, paragraphe 1, peuvent toutefois également être compris en ce sens que sont autorisés les transferts vers des pays dont le niveau de protection est déclaré inadéquat dès lors que l'autoévaluation du caractère adéquat réalisée par le responsable du traitement et/ou le sous-traitant donne un résultat satisfaisant et que des garanties appropriées ont été convenues. Le législateur européen est donc prié d'adapter les dispositions de manière à ce que l'on sache clairement quelles seraient les conséquences des décisions négatives relatives au caractère adéquat du niveau de protection et la manière dont elles fonctionneraient dans la pratique.

Transferts moyennant des garanties appropriées

La directive prévoit, à l'article 35, la possibilité de transférer des données à caractère personnel vers des pays tiers ou des organisations internationales alors que la Commission n'a pas encore adopté de décision quant au caractère adéquat du niveau de protection. Le groupe de travail estime que si ces transferts sont effectués sur le fondement d'une autoévaluation,

l'autorité compétente doit veiller à ce que les garanties appropriées aient été prévues dans un instrument juridiquement contraignant. En outre, le groupe de travail estime que les éléments énoncés à l'article 26, paragraphe 2, de la directive 95/46/CE doivent être inclus et qu'il devrait au minimum en être tenu compte lors de l'autoévaluation. Le processus aboutissant à l'autoévaluation doit être documenté et la documentation doit être mise à la disposition des autorités chargées de la protection des données si elles en font la demande.

Dérogations

Le groupe de travail s'inquiète des dérogations prévues pour le transfert de données à caractère personnel en l'absence de décision relative au caractère adéquat du niveau de protection ou de garanties appropriées (article 36), et en particulier de celles énoncées aux points c), d) et e). Ces exceptions rendraient possibles de nombreux transferts internationaux dans des cas particuliers, dès lors qu'ils sont «nécessaires». Il faut préciser que toute dérogation doit être interprétée de manière restrictive, de sorte que les transferts effectués sur ce fondement constituent une exception plutôt que la norme. Il faudrait également éviter que le libellé des dispositions puisse signifier que le simple fait de déclarer, sans autre explication, que le transfert visé doit être jugé nécessaire suffit pour invoquer ces dérogations, et qu'il autorise ainsi de nombreux transferts internationaux effectués au cas par cas, en l'absence de toute garantie relative à la protection des données à caractère personnel relatives à la personne concernée. Le groupe de travail estime dès lors que le libellé de l'article 36, points c), d) et e) devrait restreindre la possibilité de transferts internationaux dans des cas particuliers.

En outre, le groupe de travail note l'absence d'obligation destinée à garantir que soit documenté le recours à l'une quelconque des dérogations prévues à l'article 36. Cela serait pour le contrôleur difficile, voire impossible, de vérifier si les conditions auxquelles les dérogations sont subordonnées ont bien été remplies par le responsable du traitement et/ou le sous-traitant. Nous proposons donc d'inclure cette obligation en ajoutant: «*2. Le recours à ces dérogations doit être documenté et la documentation doit être mise à la disposition de l'autorité de contrôle si elle en fait la demande*».

Pour finir et d'une manière générale, en ce qui concerne les transferts internationaux pour lesquels aucune décision relative au caractère adéquat du niveau de protection n'est disponible, le groupe de travail estime que les États membres devraient pouvoir décider de l'opportunité de faire intervenir les autorités chargées de la protection des données dans les transferts internationaux et de la mesure de leur intervention.

<u>Pouvoirs des autorités chargées de la protection des données et coopération</u>

Le groupe de travail regrette que les dispositions portant sur les pouvoirs des autorités chargées de la protection des données ne soient pas très détaillées, ni cohérentes avec celles du règlement. Plus particulièrement, la directive ne comporte aucune disposition relative à l'accès aux locaux, contrairement au règlement. La capacité conférée à l'autorité de contrôle d'accéder aux locaux du responsable du traitement lorsque cela est nécessaire devrait s'appliquer à tous les secteurs.

La directive prévoit une assistance mutuelle entre les autorités chargées de la protection des données, sans toutefois mentionner les délais prévus dans le règlement. Il risque d'y avoir une incohérence et il devrait être tenu compte, pour les deux instruments, de l'avis donné sur les délais prévus dans le règlement. De même, pour veiller à la cohérence des deux instruments,

la directive devrait inclure offrir la possibilité aux autorités chargées de la protection des données de participer à des opérations conjointes.

Éléments manquants

Le groupe de travail regrette, dans la directive, l'absence de dispositions sur la fixation de délais, le contrôle et d'autres garanties, comme la limitation de l'utilisation des données pour les infractions graves, etc. Le groupe de travail prend note de l'article 37 qui prévoit l'obligation pour le responsable du traitement d'informer le destinataire de toute limitation du traitement et de prendre toutes les mesures raisonnables afin de garantir que ces limitations soient respectées. Toutefois, l'article 37 ne s'applique qu'aux transferts vers des pays tiers. Aucune indication n'est fournie sur les raisons de l'absence, dans la directive, d'une règle similaire pour le transfert de données à caractère personnel entre États membres de l'Union. Dans ce cas, les États membres destinataires devraient également être tenus de respecter toute limitation de traitement imposée par l'État membre effectuant le transfert. Le groupe de travail est surpris que la directive fasse, à cet égard, un pas en arrière par rapport à la décision-cadre 2008/977/JAI.

Le groupe de travail note l'absence d'obligation pour les autorités compétentes qui ont transmis des données d'informer le destinataire que les données transmises étaient incorrectes ou avaient été transmises de manière illicite. Cette obligation est cruciale dans un domaine où les informations de nature répressive circulent librement. L'article 39, paragraphe 2, offre aux États membres la possibilité de décider que l'autorité chargée de la protection des données qui contrôle l'application du règlement soit la même que celle qui contrôle l'application de la directive. Compte tenu des situations nationales, en particulier dans les pays disposant d'autorités locales chargées de la protection des données, le groupe de travail préférerait en effet qu'une seule autorité chargée de la protection des données soit responsable du contrôle du respect des deux instruments. Cela assurerait une cohérence dans l'application des règles.

Pour finir, le groupe de travail regrette que la directive ne comporte aucune disposition sur le transfert vers des entités privées ou d'autres autorités qui ne sont pas considérées comme des autorités compétentes au titre de la directive. Dès lors, le groupe de travail demande instamment au législateur européen d'introduire une disposition autorisant le transfert de données de nature répressive vers des entités privées uniquement dans des circonstances strictement définies par la législation.

Fait à Bruxelles, le 23 mars 2012

Pour le groupe de travail
Le président
Jacob KOHNSTAMM

L’autorité belge chargée de la protection des données et l’autorité roumaine chargée de la protection des données ont choisi de s’abstenir lors du vote au seul motif qu’elles n’approuvent pas le choix d’un règlement en tant qu’instrument juridique approprié.

L’autorité tchèque chargée de la protection des données s’est également abstenue lors du vote.

L’autorité estonienne chargée de la protection des données a voté contre l’avis car elle doute que le train de réformes proposé concorde avec les objectifs déclarés. Elle y relève trop d’éléments fondamentaux déconcertants, comme:

1) l’absence d’analyse d’impact appropriée (avis négatif du comité d'analyses d’impact),
2) la forme adoptée d’un règlement directement applicable pour une législation-cadre,
3) des charges administratives plus lourdes,
4) l’étendue de la législation déléguée,
5) l’affaiblissement des autorités nationales chargées de la protection des données, le fait que la protection de droits comportant une contrainte de temps en matière de respect de la vie privée aille plus loin, la prolongation de mesures relatives à la protection,
6) la question de la compétence dans la proposition de directive sur la protection des données dans le domaine de la police et la justice pénale,
7) la contradiction avec le principe de subsidiarité.

Par conséquent, l’autorité estonienne chargée de la protection des données ne peut marquer son accord avec les conclusions principales:

1) la proposition de règlement est trop faible pour qu’elle puisse adopter une «position globalement positive»,
2) nous ne pensons pas que la proposition de directive sur la protection des données dans le domaine de la police et la justice soit trop modeste. Nous pensons qu’elle va trop loin en raison l'absence de compétence législative dans le droit procédural national.