I

(Résolutions, recommandations et avis)

AVIS

CONTRÔLEUR EUROPÉEN DE LA PROTECTION DES DONNÉES

Avis du contrôleur européen de la protection des données sur la communication de la Commission au Parlement européen, au Conseil, au Comité économique et social et au Comité des régions intitulée — «Une approche globale de la protection des données à caractère personnel dans l'Union européenne»

(2011/C 181/01)

LE CONTRÔLEUR EUROPÉEN DE LA PROTECTION DES DONNÉES,

vu le traité sur le fonctionnement de l'Union européenne, et notamment son article 16,

vu la Charte des droits fondamentaux de l'Union européenne, et notamment ses articles 7 et 8,

vu la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données [1],

vu le règlement (CE) nº 45/2001 du Parlement européen et du Conseil du 18 décembre 2000 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données [2], et notamment son article 41,

A ADOPTÉ L'AVIS SUIVANT:

A. PARTIE GÉNÉRALE

1. Introduction

1.1. *Une première évaluation générale*

1. Le 4 novembre 2010, la Commission a adopté une communication intitulée «Une approche globale de la protection des données à caractère personnel dans l'Union européenne» (ci-après «la communication») [3]. Cette communication a été envoyée au CEPD pour consultation, lequel remercie la Commission de l'avoir consulté comme le prévoit l'article 41 du règlement (CE) nº 45/2001. Avant l'adoption de la communication, le CEPD a d'ores et déjà eu la possibilité de formuler des observations informelles, dont certaines ont été prises en considération dans la version finale du document.

2. La communication expose l'approche suivie par la Commission concernant la révision du système juridique de l'UE pour la protection des données à caractère personnel dans tous les domaines d'activités de l'Union, l'accent étant placé en particulier sur les défis résultant de la mondialisation et des nouvelles technologies [4].

3. Le CEPD approuve la communication de manière générale, étant convaincu qu'une révision du cadre juridique actuel pour la protection des données dans l'UE est nécessaire pour garantir une protection efficace dans une société de l'information en développement. Dans son avis du 25 juillet 2007 sur la mise en œuvre de la directive relative à la protection des données [5], il concluait d'ores et déjà qu'à long terme, il était inévitable que la directive 95/46/CE soit modifiée.

4. La communication représente un pas important vers cette évolution législative, laquelle constituerait l'évolution la plus importante dans le domaine de la protection des données de l'UE depuis l'adoption de la directive 95/46/CE, qui est généralement considérée comme la base principale pour la protection des données au sein de l'Union européenne (et à une échelle plus vaste au sein de l'Espace économique européen).

5. Elle établit le cadre adéquat pour une réévaluation ciblée, notamment parce qu'elle recense — de manière générale — les principaux problèmes et défis. Le CEPD partage l'avis de la Commission selon lequel un système solide de protection des données restera nécessaire à l'avenir, du fait que les principes généraux existants dans le domaine de la protection des données resteront valables dans une société soumise à des changements fondamentaux liés à des évolutions technologiques rapides et à la mondialisation. Cela requiert de revoir les dispositions législatives existantes.

[1] JO L 281 du 23.11.1995, p. 31.
[2] JO L 8 du 12.1.2001, p. 1.
[3] COM(2010) 609 final.
[4] Voir p. 5 de la communication, premier paragraphe.
[5] Avis du contrôleur européen de la protection des données du 25 juillet 2007 sur la communication de la Commission au Parlement européen et au Conseil relative au suivi du programme de travail pour une meilleure mise en application de la directive sur la protection des données, (JO C 255 du 27.10.2007, p. 1).

6. La communication souligne à raison que les défis sont de taille, appuyée en cela par le CEPD, qui ajoute qu'en conséquence, les solutions proposées devraient être pareillement ambitieuses et garantir une meilleure protection.

1.2. *L'objectif de l'avis*

7. Le présent avis évalue les solutions proposées dans la communication sur la base de ces deux critères: l'ambition et l'efficacité. Ses perspectives sont généralement positives. Le CEPD soutient la communication, mais se montre critique sur certains aspects qui, selon lui, réclament plus d'ambition en vue d'un système plus efficace.

8. Le CEPD vise, par cet avis, à contribuer à l'approfondissement du cadre juridique relatif à la protection des données. Il attend avec impatience la proposition de la Commission, prévue mi-2011, et espère que ses suggestions seront prises en considération dans le texte de cette dernière. Il note par ailleurs que la communication semble exclure certains domaines, tels que le traitement de données par les institutions et organes de l'UE, de l'instrument général. Si la Commission décidait précisément d'exclure certains domaines à ce stade — ce que le CEPD regretterait —, il la prie instamment de s'engager à élaborer une architecture complète à court terme, dans un délai déterminé.

1.3. *Le fondement du présent avis*

9. Le présent avis n'est pas le premier de ce type. Il est basé sur des positions adoptées précédemment par le CEPD et les autorités européennes chargées de la protection des données à diverses occasions. Il convient notamment de souligner que dans l'avis du CEPD du 25 juillet 2007 susmentionné, quelques éléments majeurs à modifier à l'avenir ont été déterminés et développés ([6]). Cet avis repose aussi sur des discussions avec d'autres parties prenantes dans les domaines du respect de la vie privée et de la protection des données. Leurs contributions ont été très utiles tant pour la communication que pour le présent avis. Sous ce rapport, on peut conclure qu'il existe une certaine synergie sur la façon d'assurer une protection des données plus efficace.

10. Un autre fondement important du présent avis est le document intitulé «L'avenir de la protection de la vie privée», contribution conjointe du groupe de travail «Article 29» sur la protection des données et du groupe «Police et justice» à la consultation lancée par la Commission en 2009 (ci-après le «document des groupes de travail sur l'avenir de la protection de la vie privée») ([7]).

11. Plus récemment, lors d'une conférence de presse donnée le 15 novembre 2010, le CEPD a fait part de ses premières remarques concernant la communication. Le présent avis expose les opinions d'ordre général émises à cette occasion ([8]).

12. Enfin, le présent avis se base sur plusieurs avis précédents du CEPD, ainsi que sur des documents du groupe de travail «Article 29» sur la protection des données. Les références à ces avis et documents sont mentionnées, si nécessaire, à divers endroits du présent avis.

2. **Contexte**

13. La révision des règles en matière de protection des données a lieu à un moment historique crucial. La communication décrit le contexte de manière très détaillée et convaincante. Sur la base de cette description, le CEPD met en évidence les quatre principaux facteurs déterminant l'environnement dans lequel la révision est réalisée.

14. Le premier facteur est le développement technologique. Les technologies ont évolué depuis l'élaboration et l'adoption de la directive 95/46/CE. Les phénomènes technologiques comme l'informatique en nuage, la publicité comportementale, les réseaux sociaux, les péages automatiques et les appareils de géolocalisation ont révolutionné la façon dont les données sont traitées et posent d'énormes défis pour la protection des données, qu'une révision des règles européennes en la matière devra relever de manière effective.

15. Le deuxième facteur est la mondialisation. L'abolition progressive des obstacles commerciaux a conféré aux entreprises une dimension internationale sans cesse croissante. Les traitements et les transferts internationaux de données transfrontières ont considérablement augmenté ces dernières années. En outre, le traitement de données est devenu omniprésent du fait des technologies de l'information et de la communication: l'internet et l'informatique en nuage ont permis de délocaliser le traitement de grandes quantités de données à l'échelle mondiale. On a également observé, au cours de la dernière décennie, à une intensification des activités policières et judiciaires internationales en faveur de la lutte contre le terrorisme et les autres formes de criminalité organisée internationale, à l'aide d'un échange massif d'informations à des fins répressives. Tout ceci souligne la nécessité d'un examen approfondi des modalités à mettre en œuvre pour garantir efficacement la protection des données à caractère

([6]) En particulier (voir le point 77 du présent avis): il n'est pas nécessaire de modifier les principes existants, mais il est indispensable de prendre d'autres dispositions administratives; le vaste champ d'application de la législation sur la protection des données applicable à toute utilisation de données à caractère personnel ne devrait pas être modifié; cette législation devrait permettre l'adoption d'une approche équilibrée dans des cas concrets, ainsi que la définition de priorités par les autorités de la protection des données; le système devrait s'appliquer totalement à l'utilisation de données à caractère personnel à des fins répressives, bien que des mesures supplémentaires adéquates puissent s'avérer nécessaires pour traiter certains problèmes particuliers dans ce domaine.

([7]) Document WP 168 (http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp168_fr.pdf). Son principal message est qu'un changement législatif est une bonne occasion d'éclaircir certaines règles et certains principes clés (p. ex. le consentement, la transparence), d'introduire de nouveaux principes (p. ex. la prise en compte du respect de la vie privée dès la conception, la responsabilité), de renforcer l'efficacité du système par la modernisation des dispositions existantes (p. ex. en limitant les exigences existantes en matière de notification) et d'intégrer tous les éléments dans un seul cadre juridique global (y compris la coopération policière et judiciaire).

([8]) Les points de discussion pour la conférence de presse sont disponibles sur le site du CEPD, à l'adresse suivante: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2010/10-11-15_Press_conf_speaking_points_PHBG_EN.pdf

personnel dans un contexte de mondialisation sans entraver excessivement les activités de traitement internationales.

16. Le troisième facteur est le traité de Lisbonne. L'entrée en vigueur du traité marque une nouvelle ère pour la protection des données. L'article 16 TFUE prévoit non seulement un droit individuel pour la personne concernée, mais fournit également une base juridique directe pour une solide législation en matière de protection des données à l'échelle de l'UE. Par ailleurs, l'abolition de la structure en piliers oblige le Parlement européen et le Conseil à garantir la protection des données dans tous les domaines du droit européen. En d'autres termes, elle permet la mise en place d'un cadre juridique global pour la protection des données qui soit applicable au secteur privé, au secteur public dans les États membres et aux institutions et organes de l'UE. Le programme de Stockholm ([9]) souligne avec cohérence, à cet égard, que l'Union doit élaborer une stratégie globale afin de protéger les données au sein de l'UE et dans le cadre de ses relations avec d'autres pays.

17. Le quatrième facteur est constitué par les évolutions qui ont lieu en parallèle dans le contexte des organisations internationales. Plusieurs débats sont actuellement en cours sur la modernisation des instruments juridiques existants pour la protection des données. Il convient de noter, à cet égard, les réflexions menées actuellement en relation avec la future révision de la convention 108 du Conseil de l'Europe ([10]) et des lignes directrices de l'OCDE concernant la protection de la vie privée ([11]). Une autre évolution importante concerne l'adoption de normes internationales sur la protection des données à caractère personnel et de la vie privée, qui pourrait déboucher sur l'adoption d'un instrument mondial contraignant sur la protection des données. Toutes ces initiatives méritent notre soutien total. Leur objectif commun devrait être de garantir une protection efficace et constante dans un environnement mondialisé et régi par les technologies.

3. **Principales perspectives**

3.1. *La protection des données favorise la confiance et doit soutenir les autres intérêts (publics)*

18. L'importance accordée à la protection des données dans le cadre du traité de Lisbonne, en particulier à l'article 8 de la Charte des droits fondamentaux de l'Union et à l'article 16 TFUE, ainsi que par le lien étroit établi avec l'article 7 de la charte, a eu pour conséquence nécessaire la création d'un cadre solide pour la protection des données ([12]).

19. Toutefois, ce type de cadre sert également des intérêts publics et privés plus vastes dans une société de l'information caractérisée par l'omniprésence du traitement de données. La protection des données favorise la confiance et la confiance est un élément essentiel au bon fonctionnement de notre société. Il est essentiel que les dispositions visant à garantir la protection des données soient conçues, autant que possible, de manière à soutenir activement plutôt qu'à limiter d'autres droits et intérêts légitimes.

20. Parmi les autres intérêts légitimes importants figurent une économie européenne solide, la sécurité des personnes et la responsabilisation des gouvernements.

21. Le développement économique dans l'UE va de pair avec l'introduction et la commercialisation de nouvelles technologies et de nouveaux services. Dans la société de l'information, l'émergence et le déploiement de technologies de l'information et de la communication et de services dans ce secteur dépendent de la confiance. En l'absence de confiance vis-à-vis des TIC, le succès de ces dernières est fortement compromis ([13]). Et les citoyens n'auront confiance dans les TIC que si leurs données sont efficacement protégées. Par conséquent, la protection des données devrait être automatiquement garantie pour toutes les technologies et tous les services. Un cadre solide pour la protection des données favorise l'économie européenne, à condition que ce cadre soit non seulement solide mais aussi adapté. La poursuite de l'harmonisation dans l'UE et la réduction des charges administratives à cet égard sont essentielles (voir le chapitre 5 du présent avis).

22. La nécessité d'équilibrer protection de la vie privée et sécurité a été souvent discutée ces dernières années, en particulier en relation avec les instruments pour le traitement et l'échange de données dans le domaine de la coopération policière et judiciaire ([14]). La protection des données était souvent perçue à tort comme un obstacle à la protection totale de la sécurité physique des personnes ([15]), ou au moins comme une condition inévitable à remplir par les autorités répressives. Mais ce serait oublier qu'un cadre solide pour la protection des données peut renforcer la sécurité. Les principes de protection des données (appliqués correctement) contraignent les contrôleurs à s'assurer que les informations sont exactes et à jour et que les données à caractère personnel non nécessaires à des fins de répression sont effacées des systèmes. L'on peut pareillement mettre l'accent sur les obligations d'appliquer des mesures technologiques et organisationnelles pour garantir la sécurité des systèmes, par

([9]) Le programme de Stockholm — Une Europe ouverte et sûre qui sert et protège les citoyens, (JO C 115 du 4.5.2010, p. 1), p. 10.

([10]) Convention 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, STCE n° 108, 28 janvier 1981.

([11]) Lignes directrices de l'OCDE sur la protection de la vie privée et les flux transfrontières de données de caractère personnel, publiées sur http://www.oecd.org

([12]) Cette importance accordée à la protection des données et le lien avec la protection de la vie privée dans la charte ont été mis en évidence par la Cour de justice dans son arrêt du 9 novembre 2010, affaires jointes C-92/09 et C-93/09, *Schecke*, non encore publié au Recueil.

([13]) Voir l'avis du CEPD du 18 mars 2010 sur la promotion de la confiance dans la société de l'information par la protection des données et de la vie privée, (JO C 280 du 16.10.2010, p. 1), para 113.

([14]) Voir p. ex. l'avis du contrôleur européen de la protection des données du 10 juillet 2009 sur la communication de la Commission au Parlement européen et au Conseil intitulée «Un espace de liberté, de sécurité et de justice au service des citoyens», (JO C 276 du 17.9.2009, p. 8).

([15]) La sécurité est une notion plus vaste que la sécurité physique, mais en tant qu'illustration des arguments avancés, elle est utilisée dans le cas présent dans son sens plus limité.

exemple en protégeant les systèmes contre tout accès ou divulgation non autorisés, comme c'est le cas dans le domaine de la protection des données.

23. En respectant les principes de protection des données, les autorités répressives se conforment au principe de l'État de droit, s'attirant ainsi la confiance des citoyens et favorisant la confiance de manière générale dans nos sociétés. La jurisprudence établie en vertu de l'article 8 de la Convention européenne des droits de l'homme permet aux autorités policières et judiciaires de traiter toutes les données pertinentes pour leurs activités, mais pas de manière illimitée. La protection des données requiert l'instauration de sauvegardes (voir le chapitre 9 du présent avis concernant la police et la justice).

24. Dans les sociétés démocratiques, les gouvernements sont responsables de tous leurs actes, notamment de l'usage de données à caractère personnel pour les différents intérêts publics qu'ils servent. Ces activités vont de la publication de données sur l'internet par souci de transparence à l'utilisation de données à l'appui des politiques en matière de santé publique, de transport ou de fiscalité, en passant par la surveillance de personnes à des fins répressives. Un cadre solide pour la protection des données permet aux gouvernements d'assumer leurs responsabilités et de rendre compte de leurs actions, dans le cadre du principe de bonne gouvernance.

3.2. *Les conséquences pour le cadre juridique de protection des données*

3.2.1. L'harmonisation doit se poursuivre

25. La communication a souligné à juste titre que l'une des faiblesses essentielles du cadre actuel résidait dans le fait qu'il laisse une marge d'appréciation trop importante aux États membres en ce qui concerne la transposition des dispositions européennes dans le droit national. Le manque d'harmonisation a des répercussions négatives dans une société de l'information où les frontières physiques entre les États membres perdent chaque jour un peu plus de leur raison d'être (voir le chapitre 5 du présent avis).

3.2.2. Les principes généraux de la protection des données restent valables

26. Une première raison, plus formelle, pour laquelle les principes généraux de la protection des données ne doivent ni ne peuvent être modifiés est de nature juridique. Ces principes sont établis par la convention 108 du Conseil de l'Europe, qui est contraignante pour tous les États membres. Cette convention constitue la base de la protection des données dans l'UE. En outre, certains des principes fondamentaux sont explicitement mentionnés à l'article 8 de la Charte des droits fondamentaux de l'Union. La modification de ces principes nécessiterait la modification des traités.

27. Il ne s'agit toutefois que d'une raison parmi d'autres. Il existe également des raisons importantes de ne pas modifier les principes généraux. Le CEPD est fermement convaincu qu'une société de l'information ne peut ni ne devrait fonctionner sans une protection adéquate de la vie privée et des données à caractère personnel. Dans le cas d'un traitement accru de données, la protection doit être renforcée. Une société de l'information dans laquelle des quantités massives d'information sur tout un chacun sont traitées doit reposer sur le concept de contrôle par la personne, permettant à cette dernière d'agir en tant qu'individu et de faire valoir ses libertés dans une société démocratique, notamment ses libertés d'expression et de parole.

28. Par ailleurs, il est difficile d'imaginer le contrôle par la personne en l'absence d'obligation pour les responsables du traitement de limiter le traitement en accord avec les principes de nécessité, de proportionnalité et de limitation des finalités. Il est également difficile d'imaginer un tel contrôle en l'absence de droits reconnus pour les personnes concernées, tels que les droits d'accès, de rectification, d'effacement et de verrouillage des données.

3.2.3. La perspective des droits fondamentaux

29. Le CEPD souligne que la protection des données est reconnue comme un droit fondamental. Cela ne signifie pas que la protection des données devrait toujours *prévaloir* sur d'autres droits et intérêts importants dans une société démocratique, mais cela a assurément des conséquences sur la nature et la portée de la protection qui doit être garantie dans le contexte du cadre juridique européen, de manière à s'assurer que les exigences en matière de protection des données sont toujours *adéquatement* prises en considération.

30. Ces conséquences majeures peuvent être définies comme suit:

— la protection doit être efficace. Un cadre juridique doit mettre à disposition des instruments permettant aux personnes d'exercer concrètement leurs droits;

— le cadre doit être stable sur une longue période;

— la protection doit être accordée dans toutes les circonstances et non dépendre des préférences politiques au cours d'une période déterminée;

— les limitations de l'exercice du droit peuvent être nécessaires, mais elles doivent être exceptionnelles, dûment justifiés et n'affecter en aucun cas les éléments essentiels du droit proprement dit ([16]).

Le CEPD recommande que la Commission prenne ces conséquences en considération lorsqu'il propose des solutions législatives.

3.2.4. De nouvelles dispositions législatives sont nécessaires

31. La communication se concentre à juste titre sur la nécessité de renforcer les dispositions législatives pour la protection des données. Dans ce cadre, il est utile de rappeler que dans le document des groupes de travail sur l'avenir de la protection de la vie privée ([17]), les

([16]) Voir également l'avis du contrôleur européen de la protection des données du 25 juillet 2007 sur la communication de la Commission au Parlement européen et au Conseil relative au suivi du programme de travail pour une meilleure mise en application de la directive sur la protection des données, paragraphe 17, qui se base sur la jurisprudence de la Cour européenne des droits de l'homme et de la Cour de justice.

([17]) Cf. note 7.

autorités chargées de la protection des données ont souligné la nécessité de renforcer le rôle des différents acteurs de la protection des données, en particulier les personnes concernées, les responsables du traitement et les autorités de supervision elles-mêmes.

32. Les différents acteurs semblent s'accorder pour dire que des dispositions législatives plus solides — prenant en considération les évolutions technologiques et la mondialisation — sont la clé pour une protection des données efficace et ambitieuse également à l'avenir. Comme indiqué au point 7, il s'agit là des critères pour l'évaluation par le CEPD de toute proposition de solution.

3.2.5. L'exhaustivité comme condition sine qua non

33. Comme cela a été rappelé dans la communication, la directive 95/46/CE s'applique à toutes les activités de traitement de données à caractère personnel réalisées dans les États membres, dans les secteurs tant public que privé, à l'exception des activités qui ne relèvent pas du champ d'application de l'ancien droit communautaire ([18]). Si cette exception était nécessaire sous l'ancien traité, ce n'est plus le cas depuis l'entrée en vigueur du traité de Lisbonne. En outre, elle est contraire au texte et dans tous les cas à l'esprit de l'article 16 TFUE.

34. Selon le CEPD, un instrument juridique global pour la protection des données comprenant la coopération policière et judiciaire en matière pénale est à considérer comme l'une des grandes améliorations à attendre d'un nouveau cadre juridique. Il s'agit d'une condition sine qua non pour une protection des données efficace à l'avenir.

35. Le CEPD avance les arguments suivants à l'appui de cette affirmation:

— la distinction entre les activités du secteur privé et celles des autorités répressives est de plus en plus floue. Les entités du secteur privé peuvent traiter des données qui seront utilisées en dernier lieu à des fins répressives [p. ex. les données PNR ([19])], alors que dans d'autres cas, elles sont tenues de conserver des données à des fins répressives [p. ex. la directive sur la conservation des données ([20])];

— il n'y a pas de différence fondamentale entre les autorités policières et judiciaires et les autres autorités chargées de l'application de la loi (fiscalité, douanes, antifraude, immigration) couvertes par la directive 95/46/CE;

— comme indiqué à juste titre dans la communication, l'instrument juridique de protection des données actuellement applicable aux autorités policières et judiciaires [décision-cadre 2008/977 JAI ([21])]est inadéquat;

— la plupart des États membres ont transposé la directive 95/46 CE et la convention 108 dans leurs législations nationales respectives, les rendant ainsi applicables également aux autorités policières et judiciaires.

36. L'inclusion de la police et de la justice dans l'instrument juridique général offrirait non seulement davantage de garanties au citoyen mais faciliterait également la tâche des forces de police. Le fait de devoir appliquer divers ensembles de règles est peu commode, requiert beaucoup de temps et constitue un frein pour la coopération internationale (voir le chapitre 9 du présent avis). Cela plaide aussi en faveur de l'inclusion des activités de traitement par les services de sécurité nationaux, dans la mesure où cela est possible dans le cadre actuel du droit de l'UE.

3.2.6. La neutralité technologique

37. La période qui a suivi l'adoption de la directive 95/46/CE en 1995 peut être qualifiée de technologiquement turbulente. Les évolutions technologiques et la conception de nouveaux matériels ont été fréquentes. Dans de nombreux cas, cela a entraîné des changements fondamentaux dans la façon dont les données à caractère personnel sont traitées. La société de l'information ne peut plus être considérée comme un environnement parallèle auquel les personnes peuvent participer si elles le souhaitent; elle fait à présent partie intégrante de nos vies quotidiennes. À titre d'exemple, le concept d'internet des objets ([22]) établit des liens entre les objets physiques et les informations en ligne relatives à ces objets.

38. La technologie continuera d'évoluer. Cette évolution a des conséquences pour le nouveau cadre juridique, qui doit être efficace sur une longue durée tout en ne freinant pas le développement technologique. Des dispositions juridiques technologiquement neutres sont nécessaires. Cependant, le cadre doit aussi apporter une sécurité juridique accrue aux entreprises et aux personnes, lesquelles doivent comprendre quelles sont les attentes à leur égard et doivent être capables de faire valoir leurs droits. À cette fin, les dispositions juridiques doivent être précises.

39. Selon le CEPD, un instrument juridique général pour la protection des données doit être formulé de manière technologiquement neutre, dans la mesure du possible. Cela implique que les droits et obligations des divers acteurs soient formulés dans un style général et neutre afin de garantir qu'ils restent, en principe, valables et applicables indépendamment de la technologie choisie pour traiter les données à caractère personnel. Il n'y a pas d'autre choix, étant donné le rythme actuel des avancées technologiques. Le CEPD suggère d'introduire de nouveaux droits

([18]) Le présent avis sera essentiellement axé sur l'ancien troisième pilier (coopération policière et judiciaire en matière pénale), étant donné que l'ancien deuxième pilier est non seulement un domaine plus complexe du droit de l'UE (comme le reconnaissent l'article 16 TFUE et l'article 39 UE), mais également moins pertinent pour le traitement de données.

([19]) Voir par exemple la communication de la Commission relative à la démarche globale en matière de transfert des données des dossiers passagers (PNR) aux pays tiers, COM(2010) 492 final.

([20]) La directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE (JO L 105 du 13.4.2006, p. 54).

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

([22]) Tel que défini dans «L'internet des objets — Un plan d'action pour l'Europe», COM(2009) 278 final.

«technologiquement neutres» au-delà des principes existants de protection des données qui pourraient avoir une importance spécifique dans l'environnement électronique en constante évolution (voir essentiellement les chapitres 6 et 7).

3.2.7. Le long terme: la sécurité juridique pour une période plus longue

40. La directive 95/46/CE a été la clé de voûte de la législation en matière de protection des données dans l'UE au cours de ces quinze dernières années. Elle a été transposée dans le droit des États membres et appliquée par les différents acteurs concernés. Au fil des années, son application s'est enrichie des diverses expériences pratiques et des nouvelles orientations données par la Commission, les autorités chargées de la protection des données (au niveau national et dans le cadre du groupe de travail «Article 29») et les juridictions nationales et européennes.

41. Il convient d'indiquer que ces développements nécessitent du temps et que — en particulier du fait qu'il est question d'un cadre général donnant effet à un droit fondamental — ce temps est nécessaire pour créer la sécurité et la stabilité juridiques. Un nouvel instrument juridique général doit être élaboré dans l'optique de garantir la sécurité et la stabilité juridiques sur une plus longue période, en gardant à l'esprit qu'il est très difficile de prédire la suite du développement technologique et de la mondialisation. Dans tous les cas, le CEPD soutient pleinement l'objectif d'assurer la sécurité juridique pour une plus longue période, comparable à la perspective de la directive 95/46/CE. En bref, dans les domaines où l'évolution technologique est rapide, la législation doit être stable.

3.2.8. Le court terme: faire un meilleur usage des instruments existants

42. À court terme, il est essentiel d'assurer l'efficacité des dispositions législatives existantes, en premier lieu en se concentrant sur la mise en œuvre de la législation, aux niveaux national et européen (voir le chapitre 11 du présent avis).

B. ÉLÉMENTS D'UN NOUVEAU CADRE

4. L'approche globale

43. Le CEPD soutient pleinement l'approche globale de la protection des données, qui est non seulement l'intitulé, mais également le point de départ de la communication et inclut nécessairement l'extension des règles générales sur la protection des données à la coopération policière et judiciaire en matière pénale ([23]).

44. Cependant, il note aussi que la Commission n'envisage pas d'inclure toutes les activités de traitement des données dans cet instrument juridique général. Les traitements de données réalisés par les institutions, les organes, les offices et les agences de l'UE ne seront par exemple pas inclus. La Commission déclare seulement qu'elle «évaluera la nécessité d'adapter d'autres instruments juridiques au nouveau cadre général de la protection des données».

45. Le CEPD privilégie largement l'inclusion du traitement au niveau européen dans le cadre juridique général. Il rappelle que c'était l'intention initiale de l'ancien article 286 CE, qui mentionnait pour la première fois dans un traité la question de la protection des données. Cet article prévoyait simplement que les instruments juridiques sur le traitement de données à caractère personnel s'appliqueraient également aux institutions. Plus important, un texte juridique unique permet d'éviter tout risque de disparités entre les dispositions et serait particulièrement adéquat pour l'échange de données entre le niveau européen et les entités publiques et privées des États membres. Il permettrait par ailleurs d'éviter le risque qu'après modification de la directive 95/46/CE, il n'y ait plus aucun intérêt politique à modifier le règlement (CE) nº 45/2001, ou d'accorder une priorité suffisante à cette modification pour éviter toute disparité concernant les dates d'entrée en vigueur.

46. Le CEPD prie instamment la Commission — dans le cas où elle conclurait que l'inclusion du traitement à l'échelle européenne dans l'instrument juridique général n'est pas réalisable — de s'engager à proposer une version adaptée du règlement (CE) nº 45/2001 (et non «d'évaluer la nécessité») dans les plus brefs délais et de préférence au plus tard fin 2011.

47. Il est tout aussi important que la Commission s'assure que d'autres domaines ne sont pas négligés, en particulier:

— la protection des données dans la politique étrangère et de sécurité commune, en vertu de l'article 39 TUE ([24]);

— les régimes sectoriels de protection des données applicables aux organes de l'UE comme Europol et Eurojust et aux systèmes d'information étendus, dans la mesure où ils doivent être adaptés au nouvel instrument juridique;

— la directive 2002/58 sur la vie privée et les communications électroniques, dans la mesure où elle doit être adaptée au nouvel instrument juridique.

48. Enfin, un instrument juridique général pour la protection des données peut et, probablement, doit être complété par des réglementations spécifiques et sectorielles supplémentaires, par exemple concernant la coopération policière et judiciaire, ainsi que dans d'autres domaines ([25]). Au besoin, et dans le respect du principe de subsidiarité, ces réglementations supplémentaires devraient être adoptées au niveau de l'UE. Les États membres peuvent établir des règles additionnelles dans certains domaines particuliers où ces règles s'avèrent justifiées (voir la section 5.2).

([23]) Voir la page 14 de la communication et la section 3.2.5 du présent avis.

([24]) Voir aussi l'avis du CEPD du 24 novembre 2010 sur la communication de la Commission au Parlement européen et au Conseil intitulée «La politique antiterroriste de l'UE: principales réalisations et défis à venir», point 31.

([25]) Voir aussi le document des groupes de travail sur l'avenir de la protection de la vie privée (note de bas de page 7), points 18 à 21.

5. La poursuite de l'harmonisation et de la simplification

5.1. *Le besoin d'harmonisation*

49. L'harmonisation est essentielle pour la législation européenne en matière de protection des données. La communication indique à juste titre que la protection des données a une importance considérable dans le marché intérieur car elle doit garantir la libre circulation des données à caractère personnel entre les États membres au sein de ce dernier. Toutefois, le niveau d'harmonisation prévu par la directive actuelle a été jugé insatisfaisant. La communication reconnaît qu'il s'agit de l'une des préoccupations majeures récurrentes des parties prenantes. Celles-ci soulignent notamment la nécessité de renforcer la sécurité juridique, de réduire la charge administrative et d'établir des règles de concurrence équitables pour les opérateurs économiques. Comme le constate à raison la Commission, cela vaut tout particulièrement pour les responsables du traitement de données établis dans plusieurs États membres et contraints de se conformer aux exigences (parfois divergentes) des législations nationales en matière de protection des données ([26]).

50. L'harmonisation est importante non seulement pour le marché intérieur mais aussi pour garantir une protection adéquate des données. L'article 16 TFUE dispose que «toute personne» a droit à la protection des données à caractère personnel la concernant. Pour que ce droit soit effectivement respecté, un niveau équivalent de protection doit être garanti sur tout le territoire de l'UE. Le document des groupes de travail sur l'avenir de la protection de la vie privée a relevé que plusieurs dispositions relatives aux positions des personnes concernées n'avaient pas été mises en œuvre ou interprétées de manière uniforme dans tous les États membres ([27]). Dans un monde globalisé et interconnecté, ces divergences pourraient mettre en péril ou limiter la protection des personnes.

51. Le CEPD estime que l'un des principaux objectifs de la révision est la poursuite et l'amélioration de l'harmonisation. Il salue l'engagement de la Commission à examiner les moyens de parvenir à une harmonisation accrue de la protection des données au niveau européen. Cependant, il est surpris de constater que la communication ne propose, à ce stade, aucune option concrète. Il désigne par conséquent lui-même quelques domaines nécessitant de toute urgence une convergence accrue (voir la section 5.3), qui serait réalisée non seulement en réduisant la marge de manœuvre en matière de législation nationale, mais également en empêchant toute mise en œuvre incorrecte par les États membres (voir aussi le chapitre 11) et en garantissant une mise en œuvre de la législation plus cohérente et plus coordonnée (voir aussi le chapitre 10).

([26]) Communication, p. 10.

([27]) Voir le document des groupes de travail sur l'avenir de la protection de la vie privée (note de bas de page 7), point 70. Le document fait en particulier référence aux dispositions en matière d'établissement des responsabilités et à la possibilité de réclamer une indemnisation pour préjudice immatériel.

5.2. *Réduire la marge de manœuvre en matière de transposition de la directive*

52. La directive comporte plusieurs dispositions qui sont formulées en termes généraux, générant un risque élevé de divergences en matière de transposition. Le neuvième considérant de la directive confirme explicitement que les États membres disposent d'une certaine marge de manœuvre, laquelle pourrait être à l'origine de disparités dans la transposition de la directive. Plusieurs dispositions, y compris des dispositions cruciales, ont été transposées différemment par les États membres ([28]). Cette situation n'est pas satisfaisante et il conviendrait d'œuvrer à une plus grande convergence.

53. Cela ne signifie pas que la diversité devrait être exclue systématiquement. Dans certains domaines, la flexibilité peut être nécessaire pour préserver des spécificités légitimes, des intérêts publics importants ou l'autonomie institutionnelle des États membres. Selon le CEPD, les possibilités d'écarts de mise en œuvre entre les États membres devraient être limitées en particulier aux situations spécifiques suivantes:

— Liberté d'expression: dans le cadre actuel (article 9), les États membres peuvent prévoir des exemptions et des dérogations en relation avec les traitements de données réalisés à des fins journalistiques ou à des fins d'expression artistique ou littéraire. Cette flexibilité apparaît justifiée, sous réserve, bien entendu, des limitations prévues par la charte et la CEDH, étant donné les différentes traditions et les différences culturelles qui peuvent exister dans ce domaine dans les divers États membres. Toutefois, elle n'empêcherait pas une éventuelle actualisation de l'article 9 actuel sur la base des évolutions observées sur l'internet.

— Intérêts publics spécifiques: dans le cadre actuel (article 13), les États membres peuvent adopter des mesures législatives en vue de restreindre la portée des obligations et des droits lorsqu'une telle restriction est nécessaire pour protéger des intérêts publics importants, tels que la sécurité nationale, la défense, la sécurité publique, etc. Cette compétence des États membres reste justifiée. Toutefois, le cas échéant, l'interprétation des exceptions devrait être davantage harmonisée (voir la section 9.1). En outre, le champ d'application actuel de la dérogation à l'article 6, paragraphe 1, apparaît excessivement vaste.

— Recours légaux, sanctions et procédures administratives: un cadre européen devrait déterminer les principales conditions applicables, mais dans l'état actuel du droit de l'UE, la définition des sanctions, des règles en matière de recours, des règles procédurales et des modalités d'inspection applicables au niveau national doit relever de la compétence des États membres.

([28]) Les approches divergent aussi en ce qui concerne les données traitées manuellement.

5.3. *Les domaines nécessitant une harmonisation accrue*

54. *Définitions* (article 2 de la directive 95/46/CE). Les définitions sont la pierre angulaire du système juridique et doivent être interprétées de manière uniforme dans tous les États membres, sans marge de manœuvre pour la mise en œuvre. Des disparités sont apparues dans le cadre actuel, concernant notamment la notion de responsable du traitement ([29]). Le CEPD propose d'ajouter d'autres entrées à la liste actuelle de l'article 2 afin de garantir une meilleure sécurité juridique, par exemple les termes «données anonymes», «données pseudonymes», «données judiciaires», «transfert de données» et «délégué à la protection des données».

55. *Licéité du traitement (article 5).* Le nouvel instrument juridique devrait être aussi précis que possible en ce qui concerne les éléments fondamentaux déterminant la licéité des traitements de données. L'article 5 de la directive (de même que le neuvième considérant), qui habilite les États membres à préciser les conditions dans lesquelles les traitements de données à caractère personnel sont licites, pourrait ainsi devenir inutile dans un futur cadre.

56. *Légitimité des traitements de données* (articles 7 et 8). La définition des conditions requises pour traiter des données est un élément essentiel de la législation en matière de protection des données. Les États membres ne devraient pas être autorisés à introduire, modifier ou exclure des motifs de traitement. La possibilité d'appliquer des dérogations devrait être exclue ou limitée [en particulier en ce qui concerne les données sensibles ([30])]. Dans un nouveau cadre juridique, les motifs valables de traitement de données devraient être clairement formulés, réduisant ainsi la marge d'appréciation en matière de mise en œuvre ou de mise en application. Il pourrait notamment s'avérer nécessaire de préciser la notion de consentement (voir la section 6.5). En outre, le motif reposant sur l'intérêt légitime poursuivi par le responsable du traitement [article 7, point f)] donne lieu à des interprétations sensiblement divergentes en raison de sa nature flexible. Des précisions sont indispensables. Elles pourraient également être nécessaires pour l'article 8, paragraphe 2, point b), qui autorise le traitement de données sensibles aux fins de respecter les obligations et les droits spécifiques du responsable du traitement en matière de droit du travail ([31]).

57. *Droits des personnes concernées* (articles 10 à 15). C'est l'un des domaines dans lesquels les États membres n'ont pas mis en œuvre ni interprété de manière cohérente toutes les dispositions de la directive. Les droits des personnes concernées constituent un élément central d'une protection des données efficace. La marge de manœuvre devrait par conséquent être sensiblement réduite dans ce domaine. Le CEPD recommande l'uniformisation dans toute l'UE des informations fournies aux personnes concernées par le responsable du traitement.

58. *Transferts internationaux* (articles 25 et 26). Ce domaine a donné lieu à de nombreuses critiques en raison de l'absence de pratique uniforme à travers l'UE. Les parties concernées ont critiqué le fait que les décisions de la Commission sur le caractère adéquat sont interprétées et mises en œuvre de manière très différente par les États membres. Le CEPD recommande également une meilleure harmonisation des règles d'entreprise contraignantes (voir le chapitre 9).

59. *Autorités nationales chargées de la protection des données* (article 28). Les différents États membres appliquent des règles largement différentes en ce qui concerne les autorités nationales chargées de la protection des données, en particulier concernant leur statut, leurs ressources et leurs prérogatives. L'article 28 a en partie contribué à ce manque d'harmonisation par son manque de précision ([32]) et devrait donc être formulé de manière plus précise, conformément à l'arrêt de la Cour de justice européenne dans l'affaire C-518/07 ([33]) (voir le chapitre 10).

5.4. *Simplification du système de notification*

60. Les exigences en matière de notification (articles 18 à 21 de la directive 95/46/CE) sont un autre domaine dans lequel les États membres disposent d'une marge de manœuvre importante. La communication reconnaît à juste titre qu'un système harmonisé réduirait les coûts et la charge administrative des responsables du traitement ([34]).

61. Dans ce domaine, la simplification devrait être le principal objectif poursuivi. La révision du cadre de protection des données fournit une occasion unique de simplifier et/ou réduire encore davantage le champ d'application des exigences actuelles. Ainsi que le souligne la communication, les parties intéressées s'accordent généralement à affirmer que le système de notification actuel est relativement lourd et n'apporte en soi aucune valeur ajoutée aux fins de la protection des données à caractère personnel ([35]). Le CEPD apprécie par conséquent que la Commission se soit engagée à examiner les différentes possibilités de simplification du système de notification actuel.

62. De son point de vue, cette simplification découlerait de la transition d'un système de notification systématique, sauf spécification contraire («système d'exemption»), vers un système plus ciblé. Le système d'exemption s'est avéré inefficace, en raison du manque d'harmonisation dans sa mise en œuvre au sein des divers États membres ([36]). Le CEPD suggère d'étudier les alternatives suivantes:

([29]) Voir l'avis 1/2010 du groupe de travail «Article 29» sur les notions de «responsable du traitement» et de «sous-traitant» (WP 169).

([30]) L'article 8, paragraphes 4 et 5, autorise actuellement les États membres, dans certaines conditions, à prévoir des dérogations supplémentaires pour les données sensibles.

([31]) Voir, à cet égard, le premier rapport de la Commission sur la mise en œuvre de la directive relative à la protection des données, précité, p. 14.

([32]) Document des groupes de travail sur l'avenir de la protection de la vie privée, paragraphe 87.

([33]) Affaire C-518/07, *Commission/Allemagne*, non encore publiée au Recueil.

([34]) Cf. note 26.

([35]) Cf. note 26.

([36]) Rapport du groupe de travail «Article 29» sur l'obligation de notification aux autorités nationales de contrôle, sur la meilleure utilisation des dérogations et des simplifications et sur le rôle des détachés à la protection des données dans l'Union européenne, WP 106, 2005, p. 7.

— limiter l'obligation de notification à certains types spécifiques de traitements entraînant certains risques particuliers (ces notifications pourraient donner lieu à d'autres actions, comme le contrôle préalable du traitement);

— imposer une obligation d'enregistrement simple requérant l'enregistrement des responsables du traitement (au lieu d'exiger le long processus d'enregistrement de l'ensemble des traitements de données).

En outre, un formulaire standard de notification paneuropéenne pourrait être introduit de manière à garantir des approches harmonisées concernant les informations requises.

63. La révision du système de notification actuel devrait s'effectuer sans préjudice en ce qui concerne l'amélioration des obligations de contrôle préalable pour certaines obligations de traitement susceptibles de présenter des risques spécifiques (p. ex. les systèmes d'information à grande échelle). Le CEPD est favorable à l'inclusion dans le nouvel instrument juridique d'une liste non exhaustive de cas dans lesquels ce type de contrôle préalable est requis. Le règlement (CE) n° 45/2001 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données fournit un modèle utile à cette fin ([37]).

5.5. *Un règlement, pas une directive*

64. Enfin, le CEPD estime que la révision est aussi l'occasion de redéfinir le type d'instrument juridique à utiliser pour garantir la protection des données. Un règlement, un instrument unique directement applicable dans les États membres, est le moyen le plus efficace de protéger le droit fondamental à la protection des données et de créer un véritable marché intérieur dans lequel les données à caractère personnel peuvent circuler librement et le niveau de protection est identique quel que soit le pays ou le secteur où les données sont traitées.

65. Un règlement réduirait le risque d'interprétations contradictoires et de disparités non justifiées dans la mise en œuvre et l'application de la législation. Il réduirait aussi la nécessité de déterminer le droit applicable aux traitements dans l'UE, un des aspects les plus controversés du système actuel (voir le chapitre 9).

66. Dans le domaine de la protection des données, un règlement est d'autant plus justifié que:

— l'article 16 TFUE a entériné le droit à la protection des données à caractère personnel dans les traités et envisage — voire exige — un niveau uniforme de protection des personnes sur tout le territoire de l'UE;

— le traitement de données a lieu dans un environnement électronique où les frontières internes entre les États membres ont perdu de leur importance.

([37]) Voir l'article 27 du règlement, (JO L 8 du 12.1.2001, p. 1).

67. Le choix d'un règlement comme instrument général permet, le cas échéant, d'adresser des dispositions directement aux États membres là où une certaine flexibilité est requise. Par ailleurs, il n'influence pas la compétence des États membres d'adopter, au besoin, des règles supplémentaires pour la protection des données dans le respect du droit de l'UE.

6. **Renforcer les droits des personnes**

6.1. *La nécessité de renforcer les droits*

68. Le CEPD soutient totalement la proposition formulée dans la communication de renforcer les droits des personnes, étant donné que les instruments juridiques existants ne garantissent pas pleinement la protection effective qui est requise dans un monde numérique de plus en plus complexe.

69. D'une part, l'avènement d'un monde numérique entraîne une nette augmentation de la collecte, de l'utilisation et du transfert ultérieur de données à caractère personnel par des moyens extrêmement complexes et peu transparents. Les personnes ne savent ou ne comprennent généralement pas de quelle façon cela se produit, qui collecte leurs données ni comment elles peuvent contrôler la situation. Ce phénomène est illustré par la surveillance des activités de navigation des personnes par les fournisseurs de réseaux publicitaires, qui utilisent des cookies ou autres dispositifs similaires pour proposer des publicités ciblées. Lorsque des internautes visitent des sites internet, ils ne s'attendent pas à ce qu'un tiers enregistre à distance ces visites et crée des registres d'utilisateurs sur la base d'informations qui révèlent leur style de vie ou leurs goûts.

70. D'autre part, cette évolution incite les personnes à partager volontairement leurs informations personnelles, par exemple sur des réseaux sociaux. Ceux-ci attirent des personnes de plus en plus jeunes désireuses de communiquer avec leurs pairs. Il est peu probable que les (jeunes) internautes soient conscients de la portée de la divulgation de ces informations et des effets à long terme de leurs actes.

6.2. *Une transparence accrue*

71. La transparence est vitale dans tout régime de protection des données, non seulement du fait de sa valeur intrinsèque, mais également parce qu'elle permet l'exercice d'autres principes en matière de protection des données. Les personnes ne pourront faire valoir leurs droits que si elles ont connaissance de l'existence du traitement des données.

72. Plusieurs dispositions de la directive 95/46/CE ont trait à la transparence. Les articles 10 et 11 prévoient l'obligation d'informer les personnes de la collecte de données les concernant. En outre, l'article 12 reconnaît le droit de recevoir une copie de ses propres données à caractère personnel sous une forme intelligible (droit d'accès). L'article 15 reconnaît le droit d'accès au mécanisme qui sous-tend la prise de décisions automatisées produisant des effets juridiques. Enfin, l'article 6, paragraphe 1, point a), requérant la loyauté du traitement génère une exigence de transparence. Des données à caractère personnel ne peuvent pas être traitées pour des motifs cachés ou secrets.

73. La communication suggère d'ajouter un principe général de transparence. En réaction à cette suggestion, le CEPD souligne que la notion de transparence fait déjà partie intégrante du cadre juridique actuel sur la protection des données, quoique de manière implicite. Cela peut être déduit des diverses dispositions relatives à la transparence mentionnées dans le paragraphe précédent. Selon le CEPD, il aurait pu être intéressant d'inclure un principe *explicite* de transparence, lié ou non à la disposition existante relative à la loyauté de traitement. Cela accroîtrait la sécurité juridique et confirmerait qu'un responsable du traitement doit en toutes circonstances traiter les données à caractère personnel de manière transparente, et pas uniquement lorsqu'on lui en fait la demande ou lorsqu'une disposition légale spécifique le lui impose.

74. Cependant, il est peut-être plus important de renforcer les dispositions existantes sur la transparence, dont les articles 10 et 11 de la directive 95/46/CE. Ces dispositions spécifient les éléments d'information à fournir, mais n'offrent pas de précisions concernant les modalités. Plus concrètement, le CEPD suggère de renforcer les dispositions existantes:

— en exigeant du responsable du traitement qu'il offre un accès aisé et facile à comprendre à l'information sur le traitement des données, dans un langage clair et simple ([38]). Les informations doivent être claires, visibles et bien en évidence. Ce service pourrait englober l'obligation de garantir une compréhension aisée de l'information. Pareille obligation rendrait illégales les politiques de protection de la vie privée qui sont obscures ou difficiles à comprendre;

— en exigeant de rendre l'information directement et facilement accessible aux personnes concernées. Les informations devraient par ailleurs être accessibles de façon permanente, et non être supprimées rapidement du support électronique sur lequel elles se trouvent. Cela aiderait les utilisateurs à conserver et reproduire l'information dans le futur, ce qui permettrait un accès ultérieur.

6.3. *Soutien en faveur d'une obligation de signalement des brèches de sécurité*

75. Le CEPD soutient l'introduction d'une disposition sur la notification des atteintes à la protection des données à caractère personnel dans l'instrument général, qui étende l'obligation incluse dans la directive révisée «vie privée et communications électroniques» à tous les responsables du traitement, comme proposé dans la communication. Dans le cadre de cette directive révisée, cette obligation ne s'applique qu'aux fournisseurs de services de communications électroniques (fournisseurs de services de téléphonie (dont VoIP) et d'accès à l'internet). Les autres responsables du traitement de données ne sont pas concernés par cette obligation. Or, les motifs justifiant l'instauration de cette obligation s'appliquent en tous points aux responsables du traitement autres que les fournisseurs de services de communications électroniques.

76. La notification des brèches de sécurité sert différents objectifs, le plus évident étant, comme souligné par la communication, d'informer les citoyens des risques auxquels ils sont exposés lorsque leurs données à caractère personnel ne sont plus protégées. Cela peut les inciter à prendre les mesures voulues pour réduire ces risques. Par exemple, lorsqu'ils sont avertis de failles dans la sécurité affectant leurs informations financières, ils peuvent notamment changer leurs mots de passe ou supprimer leurs comptes. En outre, ce type de notification contribue à l'application effective des autres principes et obligations visés par la directive. Les exigences de notification incitent par exemple les responsables du traitement à appliquer des mesures de sécurité plus efficaces afin de prévenir toute violation ultérieure. Les brèches de sécurité permettent aussi de renforcer la responsabilité des responsables du traitement et, plus particulièrement, de leur demander de rendre davantage compte de leurs actes (voir le chapitre 7). Enfin, elles fournissent aux autorités chargées de la protection des données un instrument de contrôle du respect des règles. La notification d'une infraction à des APD peut déboucher sur une enquête concernant l'ensemble des pratiques d'un responsable du traitement.

77. Les règles spécifiques en matière d'atteinte à la sécurité établies dans la directive «vie privée et communications électroniques» modifiée ont été longuement débattues durant la phase parlementaire du cadre législatif qui a précédé l'adoption de la directive. Lors de ce débat, les avis du groupe de travail «Article 29», du CEPD et des autres parties intéressées ont été pris en compte. Les règles adoptées reflètent les positions des différentes parties. Elles représentent un équilibre des différents intérêts: les critères sur lesquels repose l'obligation de notification sont, en principe, adéquats pour assurer la protection des personnes, mais ils n'imposent pas des exigences inutiles et excessivement lourdes.

6.4. *Renforcer le consentement*

78. L'article 7 de la directive sur la protection des données mentionne six bases juridiques pour le traitement de données à caractère personnel. Le consentement des personnes en est une. Un responsable du traitement est autorisé à traiter des données à caractère personnel dans la mesure où les personnes ont accepté, après avoir été dûment informées, que leurs données soient collectées et ultérieurement traitées.

79. Dans la pratique, les utilisateurs ne peuvent généralement qu'exercer un contrôle limité en relation avec leurs données, en particulier dans un environnement technologique. L'une des méthodes parfois utilisées est le consentement implicite, à savoir le consentement qui a été induit d'un acte d'une personne (p. ex. une personne qui utilise

([38]) Voir la communication, p. 6.

un site internet est réputée consentir à l'enregistrement de ses données à des fins de marketing) ou de son silence ou inaction (le fait de ne pas décocher une case cochée est assimilé à un consentement).

80. En vertu de la directive, un consentement n'est valable que s'il est libre, spécifique et informé. Il s'agit d'une manifestation de volonté informée par laquelle la personne concernée accepte que des données à caractère personnel la concernant fassent l'objet d'un traitement. Le consentement doit être donné de manière non équivoque.

81. Le consentement déduit d'un acte et, plus particulièrement, d'un silence ou d'une inaction est souvent équivoque. Il n'est cependant pas toujours simple de déterminer ce qui constitue un consentement authentique, non équivoque. Certains responsables du traitement exploitent cette incertitude en recourant à des méthodes qui excluent toute possibilité de donner un consentement véritable, non équivoque.

82. À la lumière des faits susmentionnés, le CEPD partage l'avis de la Commission sur la nécessité de préciser les limites du consentement et de s'assurer que seul le consentement résultant d'un comportement non équivoque est considéré comme tel. Dans ce contexte, il suggère ce qui suit ([39]):

— envisager éventuellement d'élargir le champ des situations dans lesquelles un consentement exprès est requis — actuellement limité aux données sensibles;

— adopter des règles supplémentaires en matière de consentement dans un environnement virtuel;

— adopter des règles supplémentaires en matière de consentement pour le traitement de données à des fins secondaires (c'est-à-dire lorsque le traitement est secondaire au traitement principal ou n'apparaît pas comme une évidence);

— dans un nouvel instrument législatif, adopté ou non par la Commission en vertu de l'article 290 TFUE, déterminer le type de consentement requis, par exemple, préciser le niveau de consentement à l'égard du traitement de données via des étiquettes RFID sur les produits de consommation ou d'autres techniques spécifiques.

6.5. *La portabilité des données et le droit à l'oubli*

83. La portabilité des données et le droit à l'oubli sont deux notions liées présentées dans la communication afin de renforcer les droits des personnes concernées. Ils complètent les principes déjà mentionnés dans la directive, autorisant la personne concernée à s'opposer au traitement ultérieur de ses données à caractère personnel et contraignant le responsable du traitement à effacer les informations dès qu'elles ne sont plus nécessaires au traitement.

84. Ces deux notions nouvelles présentent surtout de la valeur ajoutée dans une société de l'information, où les données sont de plus en plus enregistrées automatiquement et conservées pendant une période illimitée. La pratique montre que même dans les cas où les données sont introduites par la personne concernée elle-même, le niveau effectif de contrôle de celle-ci sur ses données est dans la pratique très limité. C'est d'autant plus vrai si l'on pense à la gigantesque mémoire que représente l'internet aujourd'hui. Par ailleurs, d'un point de vue économique, il est plus coûteux pour un responsable du traitement d'effacer des données que de les conserver. L'exercice des droits d'une personne va par conséquent à l'encontre de la tendance économique naturelle.

85. La portabilité des données et le droit à l'oubli pourraient tous deux contribuer à faire pencher la balance en faveur de la personne concernée. La première viserait à garantir à celle-ci un contrôle accru sur ses informations, tandis que le second garantirait l'élimination automatique des données après un certain temps, même si la personne concernée n'en fait pas la demande, voire n'a pas connaissance du fait que ces données avaient été enregistrées.

86. De manière plus spécifique, la portabilité des données est comprise comme étant la capacité des utilisateurs à modifier leurs préférences concernant le traitement de leurs données, en relation, plus particulièrement, avec les nouveaux services technologiques. De plus en plus, cela s'applique à des services qui induisent le stockage d'informations, y compris à caractère personnel, tels que des services de téléphonie mobile ou des services de stockage d'images, de courriels et d'autres informations, parfois à l'aide de services d'informatique en nuage.

87. Les personnes doivent pouvoir changer facilement et en toute liberté de fournisseur et transférer leurs données à caractère personnel à un autre fournisseur. Le CEPD estime que les droits existants établis dans la directive 95/46/CE pourraient être renforcés par l'inclusion d'un droit de portabilité, en particulier dans le contexte des services fournis dans une société de l'information, afin d'aider les personnes à s'assurer que les fournisseurs ou autres responsables du traitement concernés leur donnent accès à leurs informations personnelles et que les anciens fournisseurs ou autres responsables du traitement effacent ces données même s'ils souhaiteraient les conserver à des fins légitimes propres.

88. Un «droit à l'oubli» nouvellement codifié garantirait l'effacement de données à caractère personnel ou interdirait leur usage ultérieur, sans action obligatoire de la part de

([39]) Le groupe de travail «Article 29» élabore en ce moment un avis sur le «consentement», lequel pourrait déboucher sur de nouvelles suggestions.

la personne concernée, mais à la condition que ces données soient déjà stockées depuis un certain temps. En d'autres termes, les données se verraient attribuer une «date d'expiration». Ce principe est d'ores et déjà invoqué dans les procédures judiciaires nationales ou appliqué dans des secteurs spécifiques, par exemple dans le cas des fichiers des services de police, des casiers judiciaires ou des dossiers disciplinaires: en vertu de certaines législations nationales, les informations personnelles sont automatiquement effacées ou ne peuvent plus être utilisées ou divulguées, en particulier après un certain temps, sans analyse préalable réalisée au cas par cas.

89. Dans ce sens, un nouveau «droit à l'oubli» devrait être connecté à la portabilité des données. Son intérêt résiderait dans le fait qu'aucune action ni demande insistante de la part de la personne concernée ne serait nécessaire pour obtenir l'effacement de données à caractère personnel, car celui-ci aurait lieu de manière objective et automatisée. Ce n'est que dans des circonstances très spécifiques, où un besoin spécifique de conserver des données pendant une plus longue période serait établi, qu'un responsable du traitement serait autorisé à les conserver. Ce droit transférerait ainsi la charge de la preuve de la personne concernée au responsable du traitement et constituerait un paramètre de «respect de la vie privée par défaut» pour le traitement de données à caractère personnel.

90. Le CEPD estime que le droit à l'oubli pourrait être particulièrement utile dans le contexte de services de la société de l'information. Une obligation d'effacer ou de ne pas continuer de divulguer des informations après un certain temps est particulièrement utile dans les médias ou sur l'internet, surtout dans les réseaux sociaux. Elle aurait aussi son utilité dans le contexte des équipements terminaux: les données stockées sur des appareils mobiles ou des ordinateurs seraient automatiquement effacées ou verrouillées passé un certain délai, lorsque ces équipements ne sont plus en la possession des personnes concernées. Dans ce sens, le droit à l'oubli peut être traduit en une obligation de «respect de la vie privée dès la conception» («privacy by design»).

91. En résumé, le CEPD est d'avis que la portabilité des données et le droit à l'oubli sont des concepts utiles. Il pourrait être intéressant de les inclure dans l'instrument juridique, mais probablement en les limitant à l'environnement électronique.

6.6. *Le traitement de données à caractère personnel concernant des enfants*

92. Dans le cadre de la directive 95/46/CE, il n'existe pas de règles particulières concernant le traitement de données à caractère personnel relatives à des enfants. Ainsi, n'est pas reconnue la nécessité d'une protection spécifique des enfants dans des circonstances particulières, en raison de leur vulnérabilité et en raison de l'insécurité juridique occasionnée, en particulier dans les domaines suivants:

— la collecte d'informations sur des enfants et la façon dont ils doivent être informés de cette collecte;

— la façon dont le consentement des enfants est obtenu. Étant donné qu'il n'existe pas de règles spécifiques sur la façon d'obtenir le consentement d'enfants ni sur l'âge en-deçà duquel les enfants sont à considérer comme tels, ces questions sont traitées dans le cadre du droit national, qui diffère selon les États membres ([40]);

— les moyens et modalités à la disposition des enfants ou de leurs représentants légaux pour faire valoir leurs droits au titre de la directive.

93. Le CEPD considère que les intérêts spécifiques des enfants seraient mieux protégés si le nouvel instrument juridique contenait des dispositions supplémentaires, spécifiquement adaptées à la collecte et au traitement ultérieur de données relatives à des enfants. Ces dispositions offriraient aussi une sécurité juridique dans ce domaine spécifique et seraient profitables aux responsables du traitement actuellement exposés à des exigences juridiques divergentes.

94. Le CEPD propose d'inclure les dispositions suivantes dans l'instrument juridique:

— une exigence d'information à adapter aux enfants dans la mesure où elle permettrait aux enfants de comprendre plus facilement ce qu'implique la collecte de données les concernant;

— d'autres exigences d'information adaptées aux enfants, sur la façon dont les informations doivent être fournies, ainsi qu'éventuellement, sur leur contenu;

— une disposition spécifique protégeant les enfants contre la publicité comportementale;

— le principe de limitation des finalités devrait être renforcé pour les données relatives à des enfants;

— certaines catégories de données ne devraient jamais être collectées auprès d'enfants;

— une limite d'âge, en-deçà de laquelle les informations générales sur des enfants devraient être collectées uniquement avec le consentement exprès et vérifiable des parents;

— si le consentement parental est nécessaire, il serait nécessaire d'établir des règles sur la façon d'authentifier

([40]) Le consentement est généralement lié à l'âge à partir duquel les enfants peuvent être soumis à des obligations contractuelles. C'est l'âge auquel les enfants sont censés avoir atteint un certain degré de maturité. Par exemple, le droit espagnol exige d'obtenir le consentement parental pour collecter des données concernant des enfants de moins de 14 ans. Les enfants plus âgés sont réputés aptes à donner leur consentement. Au Royaume-Uni, la loi sur la protection des données ne mentionne aucun âge ou limite d'âge particulier. Cependant, l'autorité britannique de la protection des données a conclu que les enfants de plus de 12 ans pouvaient donner leur consentement, ce qui n'est pas le cas pour les enfants de moins de 12 ans, pour lesquels des données ne peuvent être collectées qu'après avoir obtenu l'autorisation d'un parent ou d'un tuteur.

l'âge de l'enfant, c'est-à-dire sur la façon de vérifier qu'un enfant est mineur d'âge et que les parents ont donné leur consentement. Dans ce domaine, l'UE peut s'inspirer d'autres pays comme les États-Unis ([41]).

6.7. *Les mécanismes de recours collectif*

95. Renforcer les droits des personnes en tant que tels serait inutile, en l'absence de mécanismes procéduraux efficaces pour opposer ces droits. Dans ce contexte, le CEPD recommande l'introduction dans la législation de l'UE de mécanismes de recours collectif en cas de violation des règles en matière de protection des données. Les mécanismes de recours collectif permettant à des groupes de citoyens de combiner leurs différentes plaintes en un seul recours pourraient constituer un outil très efficace pour faciliter l'application de ces règles ([42]). Cette innovation est également soutenue par les autorités chargées de la protection des données dans le document des groupes de travail sur l'avenir de la protection de la vie privée.

96. Dans le cas de répercussions mineures, il est peu probable que les victimes d'une violation des règles relatives à la protection des données intentent des recours individuels contre les responsables du traitement, en raison des coûts, des retards, des incertitudes, des risques et des charges auxquels elles seraient exposées. Ces difficultés pourraient être éliminées ou considérablement réduites si un système de recours collectif était en place, habilitant les victimes de violations à regrouper leurs plaintes individuelles en un seul recours. Le CEPD serait également favorable à l'habilitation des entités qualifiées, telles que les associations de consommateurs ou les organes publics, à engager des actions en dommages et intérêts au nom des victimes. Ces actions ne porteraient pas atteinte au droit de la personne concernée d'intenter un recours à titre individuel.

97. Les recours collectifs sont importants non seulement pour garantir une indemnisation totale ou toute autre mesure de réparation, mais aussi parce qu'ils constituent indirectement un moyen de dissuasion. Le risque de devoir supporter les frais d'une lourde indemnisation collective dans le cadre de telles actions inciterait d'autant plus les responsables du traitement à adopter des mesures efficaces pour s'assurer qu'ils respectent les règles. Sous ce rapport, de meilleures actions de contrôle de l'application des règles par des particuliers au moyen de mécanismes de recours collectif complèteraient les mesures de contrôle des organes publics.

98. La communication ne se prononce pas sur ce sujet. Le CEPD a connaissance du débat actuellement en cours au niveau européen concernant l'introduction du mécanisme de recours collectif de consommateurs. Il est également conscient du risque d'abus que ces mécanismes peuvent entraîner sur la base de l'expérience recueillie dans d'autres systèmes juridiques. Toutefois, ces facteurs ne constituent pas à ses yeux des arguments suffisants pour rejeter ou reporter leur introduction dans la législation sur la protection des données, au vu des bienfaits qui en découleraient ([43]).

7. **Renforcer le rôle des organisations/responsables du traitement**

7.1. *Généralités*

99. Le CEPD est d'avis qu'outre le renforcement des droits des personnes, un instrument juridique moderne pour la protection des données doit contenir les instruments nécessaires pour accroître la responsabilité des responsables du traitement. De manière plus spécifique, le cadre doit prévoir des dispositions qui motivent ces derniers, dans le secteur tant public que privé, à inclure à titre préventif des mesures de protection des données dans leurs processus opérationnels. Ces instruments seraient utiles, premièrement, parce que, comme mentionné précédemment, les évolutions technologiques ont considérablement intensifié la collecte, l'utilisation et le transfert ultérieur de données à caractère personnel, accentuant le risque d'atteinte à la vie privée et à la protection des données à caractère personnel, qu'il convient de compenser de manière efficace. Deuxièmement, le cadre actuel ne prévoit pas — excepté dans de rares dispositions précisément définies (voir plus bas) — de tels instruments, et les responsables du traitement pourraient adopter une approche *réactive* à l'égard de la protection des données et de la vie privée et ne prendre des mesures qu'après l'apparition d'un problème. Cette approche est confirmée dans les statistiques, qui indiquent comme problèmes récurrents des pratiques de contrôle médiocres et des pertes de données.

100. Selon le CEPD, le cadre existant ne suffit pas pour protéger les données à caractère personnel de manière efficace dans les conditions actuelles et futures. Plus les risques sont élevés, plus il est nécessaire d'appliquer des mesures concrètes qui protègent l'information sur le plan pratique et garantissent une protection effective. À moins que ces mesures préventives soient appliquées de facto, des erreurs, des contretemps et des négligences continueront de se produire, mettant en péril la protection de la vie privée dans cette société de plus en plus numérique. À cette fin, le CEPD propose les mesures suivantes.

7.2. *Renforcer la responsabilité des responsables du traitement*

101. Le CEPD recommande d'inclure dans l'instrument juridique une nouvelle disposition exigeant des responsables du traitement qu'ils appliquent des mesures adéquates et efficaces garantissant le respect des principes et obligations prévus par l'instrument juridique et démontrent sur demande que ces principes et obligations sont bel et bien respectés.

([41]) Aux États-Unis, la loi sur la protection de la vie privée en ligne des enfants (COPPA) requiert des opérateurs de sites commerciaux ou de services en ligne destinés aux enfants de moins de 13 ans qu'ils obtiennent le consentement des parents avant de collecter des informations personnelles; elle impose également aux opérateurs de sites commerciaux destinés au grand public de garder à l'esprit que certains visiteurs sont des enfants.

([42]) Voir aussi l'avis du contrôleur européen de la protection des données du 25 juillet 2007 sur la communication de la Commission au Parlement européen et au Conseil relative au suivi du programme de travail pour une meilleure mise en application de la directive sur la protection des données, (JO C 255 du 27.10.2007, p. 10).

([43]) Certaines législations nationales prévoient déjà des mécanismes similaires.

102. Ce type de disposition n'est pas entièrement nouveau. L'article 6, paragraphe 2, de la directive 95/46/CE fait référence aux principes relatifs à la qualité des données et mentionne qu'«il incombe au responsable du traitement d'assurer le respect du paragraphe 1». Pareillement, l'article 17, paragraphe 1, impose aux responsables du traitement de mettre en œuvre des mesures techniques et d'organisation. Toutefois, ces dispositions ont un champ d'application limité. L'insertion d'une disposition générale sur la responsabilisation inciterait les responsables du traitement à mettre en place des mesures préventives afin de se conformer à toutes les règles de la législation relative à la protection des données.

103. Une disposition en matière de responsabilisation engagerait les responsables du traitement à mettre en place des mécanismes et des systèmes de contrôle internes garantissant le respect des principes et obligations établis par le cadre. Cela impliquerait, par exemple, d'associer les cadres supérieurs à l'élaboration des politiques en matière de protection des données, d'établir un plan des procédures afin de garantir l'identification requise de tous les traitements, d'appliquer des politiques de protection des données qui soient contraignantes et continuellement révisées et mises à jour afin de couvrir les nouveaux traitements, d'observer les principes en matière de qualité des données, de notification, de sécurité, d'accès, etc. Cela impliquerait par ailleurs que les responsables du traitement conservent des preuves leur permettant d'établir leur conformité si les autorités compétentes leur en font la demande. L'apport de la preuve de la conformité au grand public devrait également être rendue obligatoire dans certains cas. Il pourrait, à cette fin, être par exemple demandé aux responsables du traitement d'inclure la protection des données dans leurs rapports (annuels) publics, lorsque ces rapports sont obligatoires pour d'autres motifs.

104. À l'évidence, les types de mesures internes et externes à mettre en œuvre doivent être appropriés et dépendre des faits et circonstances de chaque cas particulier. Cela fait une différence si un responsable du traitement traite quelques centaines de dossiers de clients ne mentionnant que des noms et des adresses ou s'il traite les dossiers de millions de patients, dont leur historique médical. Il en va de même pour les méthodes spécifiques d'évaluation de l'efficacité des mesures prises. Il convient de faire preuve de flexibilité.

105. L'instrument juridique complet et global de protection des données ne devrait pas établir les exigences spécifiques en matière de responsabilisation, mais uniquement ses éléments essentiels. La communication prévoit certains éléments pour renforcer la responsabilité («accountability») des responsables du traitement, qui sont particulièrement bienvenus. De manière plus spécifique, le CEPD appuie totalement l'idée de rendre obligatoires, dans certaines conditions, la désignation d'un délégué à la protection des données et la réalisation d'évaluations d'impact à l'égard de la protection de la vie privée.

106. En outre, le CEPD recommande de déléguer des pouvoirs à la Commission en vertu de l'article 290 TFUE afin de compléter les exigences fondamentales nécessaires pour assurer le respect de la norme en matière de responsabilisation. L'utilisation de ces pouvoirs améliorerait la sécurité juridique pour les responsables du traitement et permettrait d'harmoniser la conformité à travers l'UE. Lors de l'élaboration de ces instruments spécifiques, le groupe de travail «Article 29» et le CEPD devraient être consultés.

107. Enfin, les mesures de responsabilisation concrètes requises des responsables du traitement pourraient également être imposées par les autorités chargées de la protection des données dans le cadre de leurs compétences en matière de contrôle de l'application des règles. Ces autorités devraient pour cela se voir attribuer de nouveaux pouvoirs leur permettant d'imposer des mesures de réparation ou des sanctions. Il pourrait s'agir de mettre en place des programmes de conformité internes, d'appliquer le principe de respect de la vie privée dès la conception («privacy by design») pour certains produits et services spécifiques, etc. Les mesures correctives imposées doivent être appropriées, proportionnées et efficaces aux fins de la mise en conformité avec les normes légales applicables et exécutoires.

7.3. Le respect de la vie privée dès la conception («privacy by design»)

108. Le principe de respect de la vie privée dès la conception fait référence à l'intégration des aspects relatifs à la protection des données et de la vie privée dès la phase de conception de nouveaux produits, services et procédures qui engendrent le traitement de données à caractère personnel. Selon le CEPD, il s'agit d'un élément du principe de responsabilité. Dans la même logique, les responsables du traitement devraient aussi démontrer qu'ils ont appliqué le principe de respect de la vie privée dès la conception, le cas échéant. Récemment, la 32e conférence internationale des commissaires à la protection des données et de la vie privée a débouché sur une résolution reconnaissant la protection intégrée de la vie privée comme un élément fondamental de la protection de la vie privée. ([44])

109. La directive 95/46/CE comporte plusieurs dispositions encourageant la prise en compte du principe de respect de la vie privée dès la conception ([45]), mais ne reconnaît pas cette obligation explicitement. Le CEPD salue la reconnaissance, dans la communication, de ce principe en tant qu'instrument garantissant le respect des règles en matière de protection des données. Il suggère d'inclure une disposition contraignante établissant l'obligation d'intégrer le respect de la vie privée dès la conception, qui pourrait

([44]) Résolution sur la protection intégrée de la vie privée, adoptée lors de la 32e Conférence internationale des commissaires à la protection des données et de la vie privée, tenue à Jérusalem du 27 au 29 octobre 2010.

([45]) La directive inclut des dispositions qui, de manière indirecte, dans différentes situations, exigent l'application de ce principe. En particulier, l'article 17 prévoit que les responsables du traitement prennent des mesures techniques et d'organisation appropriées pour prévenir tout traitement de données illicite. La directive «Vie privée et communications électroniques» est plus explicite. En vertu de son article 14, paragraphe 3, «au besoin, des mesures peuvent être adoptées afin de garantir que les équipements terminaux seront construits de manière compatible avec le droit des utilisateurs de protéger et de contrôler l'utilisation de leurs données à caractère personnel, conformément à la directive 1999/5/CE et à la décision 87/95/CEE du Conseil du 22 décembre 1986 relative à la normalisation dans le domaine des technologies de l'information et des télécommunications».

s'inspirer du libellé du considérant 46 de la directive 95/46/CE. Plus précisément, cette disposition exigerait explicitement des responsables du traitement qu'ils prennent des mesures techniques et d'organisation, tant au moment de la conception du système de traitement qu'au moment du traitement lui-même, en particulier afin de garantir la protection des données à caractère personnel et de prévenir tout traitement illégal ([46]).

110. En vertu de cette disposition, les responsables du traitement seraient tenus — entre autres — de s'assurer que les systèmes de traitement des données sont conçus de manière à traiter aussi peu de données que possible, d'appliquer des paramètres de protection de la vie privée par défaut, par exemple dans les réseaux sociaux, d'interdire par défaut l'accès aux profils personnels par des tiers et de mettre en œuvre des instruments permettant aux utilisateurs de mieux protéger leurs données à caractère personnel (p. ex. contrôles d'accès, cryptage).

111. Les bienfaits d'une référence plus explicite au principe de respect de la vie privée dès la conception peuvent être résumés comme suit:

— cela mettrait en lumière l'importance du principe en tant que tel comme instrument garantissant que les processus, produits et services sont conçus dès les premiers stades dans l'optique du respect de la vie privée;

— cela réduirait les atteintes au droit du respect à la vie privée et permettrait de diminuer les collectes de données inutiles et d'habiliter les particuliers à faire de véritables choix à propos des données les concernant;

— cela permettrait d'éviter de devoir recourir à des solutions de fortune pour tenter de remédier à des problèmes qui pourraient s'avérer difficiles, voire impossibles, à résoudre;

— cela faciliterait également l'application et le contrôle du respect effectifs de ce principe par les autorités chargées de la protection des données.

112. L'effet combiné de cette obligation donnerait lieu à une hausse de la demande de produits et services conçus selon ce principe, ce qui devrait inciter davantage l'industrie à répondre à cette demande. Il conviendrait d'envisager, par ailleurs, de créer une obligation distincte qui s'appliquerait aux concepteurs et fabricants de nouveaux produits et services susceptibles d'avoir une incidence sur la protection des données et de la vie privée. Le CEPD suggère d'inclure ce type d'obligation, laquelle permettrait aux responsables du traitement de se conformer à leur propre obligation.

113. La codification du principe d'intégration du respect de la vie privée dès la conception pourrait être complétée par une disposition établissant des exigences générales en la matière s'appliquant à l'ensemble des secteurs, produits et services – par exemple des mesures d'habilitation des utilisateurs, à adopter suivant ce principe.

114. En outre, le CEPD recommande de déléguer des pouvoirs à la Commission en vertu de l'article 290 TFUE afin — le cas échéant — de compléter les exigences fondamentales en matière d'intégration du respect de la vie privée dès la conception pour certains produits et services déterminés. L'utilisation de ces pouvoirs améliorerait la sécurité juridique pour les responsables du traitement et permettrait d'harmoniser la conformité à travers l'UE. Lors de l'élaboration de ces instruments spécifiques, le groupe de travail «Article 29» et le CEPD devraient être consultés (voir dans ce sens le point 106 sur la responsabilité).

115. Enfin, les autorités chargées de la protection des données devraient être habilitées à appliquer des mesures de réparation ou des sanctions, sous les mêmes conditions restrictives que mentionné au point 107, lorsque les responsables du traitement n'ont manifestement pas pris de mesures concrètes dans des cas où elles s'imposaient.

7.4. *Les services de certification*

116. La communication reconnaît la nécessité d'examiner la possibilité de mettre en place des systèmes européens de certification pour les produits et services respectant les exigences en matière de respect de la vie privée. Le CEPD soutient pleinement cet objectif et suggère d'inclure une disposition relative à leur création et à leurs effets potentiels dans l'UE, aspect qui pourra éventuellement être développé ultérieurement dans une nouvelle législation. Cette disposition devrait compléter celles sur la responsabilité et la prise en compte du respect de la vie privée dès la conception.

117. Des mécanismes de certification volontaires permettraient de vérifier qu'un responsable du traitement a adopté les mesures requises pour se conformer aux exigences prévues par l'instrument juridique. De plus, les responsables du traitement — voire les produits ou les services — certifiés sont susceptibles d'avoir un avantage compétitif sur les autres. Ces mécanismes serviraient aussi d'appui pour les autorités chargées de la protection des données dans leur rôle de supervision et de contrôle de l'application des règles.

8. **La mondialisation et le droit applicable**

8.1. *Un besoin évident de cohérence accrue en matière de protection*

118. Comme mentionné ci-dessus au chapitre 2, le transfert de données à caractère personnel vers des pays tiers s'est considérablement accru du fait du développement de nouvelles technologies, du rôle des multinationales et de l'influence accrue des gouvernements dans le traitement et le partage de données à caractère personnel à l'échelle internationale. C'est l'une des principales raisons expliquant la nécessité de réviser le cadre juridique actuel. Par conséquent, c'est l'un des domaines dans lesquels le CEPD demande ambition et efficacité, étant donné le besoin évident d'une protection plus cohérente lors du traitement de données en dehors de l'UE.

([46]) Dans le cadre actuel, le considérant 46 encourage les responsables du traitement à mettre en œuvre ce type de mesures, mais un considérant n'a bien entendu aucun effet contraignant.

8.2. *Investir dans des règles internationales*

119. Selon le CEPD, il convient de s'investir davantage dans l'élaboration de règles internationales. Une harmonisation accrue des différents niveaux de protection des données à caractère personnel à travers le monde permettrait de mieux délimiter le fond des principes à respecter et de préciser les modalités de transferts de données. Ces règles globales devraient concilier l'exigence d'une norme élevée en matière de protection des données — y compris les éléments européens fondamentaux en matière de protection des données — et les spécificités régionales.

120. Le CEPD salue les efforts ambitieux déployés à ce stade dans le cadre de la conférence internationale des commissaires à la protection des données pour concevoir et diffuser ce que l'on appelle les «normes de Madrid», dans l'optique de les intégrer dans un instrument contraignant et d'organiser éventuellement une conférence intergouvernementale ([47]). Il invite la Commission à prendre les initiatives nécessaires pour faciliter la réalisation de cet objectif.

121. De l'avis du CEPD, il importe également de garantir la cohérence entre cette initiative en faveur de l'établissement de normes internationales, la révision actuelle du cadre européen de la protection des données et d'autres développements tels que la révision actuelle des lignes directrices de l'OCDE en matière de respect de la vie privée et de la convention 108 du Conseil de l'Europe, qui est ouverte à la signature par des pays tiers (voir également le point 17). Le CEPD estime que la Commission a un rôle spécifique à jouer à cet égard, en déterminant de quelle façon elle encouragera cette cohérence dans les négociations avec l'OCDE et le Conseil de l'Europe.

8.3. *Clarifier les critères en matière de droit applicable*

122. Etant donné qu'une cohérence totale est difficilement envisageable, il subsistera — au moins à court terme — quelques disparités entre les différentes législations au sein de l'UE et a fortiori en dehors de l'UE. Le CEPD considère qu'un nouvel instrument juridique devra préciser les critères déterminant le droit applicable et devra instaurer des mécanismes harmonisés pour la circulation des données ainsi que la notion de responsabilité des acteurs impliqués dans ces transferts.

123. Dans un premier temps, l'instrument juridique devrait garantir l'application du droit de l'UE lorsque des données à caractère personnel sont traitées dans des pays tiers, mais qu'il existe une demande justifiée d'appliquer le droit de l'UE. Un exemple illustrant cette nécessité concerne les services d'informatique en nuage non européens destinés aux résidents de l'UE. Dans un environnement où les données ne sont pas physiquement stockées et traitées dans un endroit fixe, où les fournisseurs de services et les utilisateurs situés dans des pays différents ont une influence et une possibilité d'ingérence en ce qui concerne les données, il est très difficile de déterminer à qui incombe la responsabilité d'observer quels principes en matière de protection des données. Des orientations ont été diffusées, en particulier par les autorités chargées de la protection des données, sur la façon d'interpréter et d'appliquer la directive 95/46/CE dans pareils cas, mais des orientations seules ne suffisent pas à garantir la sécurité juridique dans ce nouvel environnement.

124. Sur le territoire de l'UE, la nécessité d'une précision accrue dans le cadre juridique et d'un critère simplifié pour déterminer le droit applicable a été mise en évidence par le groupe de travail «Article 29» dans un avis récent ([48]).

125. Selon le CEPD, il serait préférable d'intégrer l'instrument juridique dans un règlement qui entraînerait l'application de règles identiques dans tous les États membres. Un règlement réduirait la nécessité de déterminer le droit applicable. C'est l'une des raisons pour lesquelles le CEPD plaide fortement en faveur de l'adoption d'un règlement. Ce type d'instrument pourrait cependant offrir aux États membres une certaine marge de manœuvre. Si le nouvel instrument laisse une marge de manœuvre importante, le CEPD suggèrerait, à l'instar du groupe de travail, l'abandon d'une application distributive des différentes législations nationales au profit d'une application centralisée d'une seule législation dans tous les États membres où un responsable du traitement est implanté. Il insiste par ailleurs pour que soient renforcées la coopération et la coordination entre les autorités chargées de la protection des données dans les dossiers et les recours transnationaux (voir le chapitre 10).

8.4. *Rationaliser les mécanismes régissant la circulation des données*

126. Le besoin de cohérence et de solides critères d'évaluation doit être pris en compte non seulement à l'égard des principes internationaux de protection des données, mais aussi à l'égard des transferts internationaux. Le CEPD soutient pleinement l'objectif de la Commission visant à rationaliser les procédures actuelles de transferts de données internationaux et à garantir une approche plus uniforme et plus cohérente vis-à-vis des pays tiers et des organisations internationales.

127. Le mécanisme régissant la circulation des données inclut à la fois les transferts du secteur privé, en particulier via des clauses contractuelles ou des règles d'entreprise contraignantes, et les transferts entre les administrations. Les règles d'entreprise contraignantes, notamment, nécessiteraient une approche plus cohérente et rationalisée. Le CEPD recommande de traiter la question des conditions relatives à ces règles de manière explicite dans le nouvel instrument juridique ([49]), en:

— reconnaissant explicitement les règles d'entreprise contraignantes comme des instruments offrant des garanties adéquates;

— définissant les principaux éléments/conditions pour l'adoption de ces règles;

([47]) Comme suggéré par la résolution sur les normes internationales, adoptée lors de la 32e Conférence internationale des commissaires à la protection des données et de la vie privée, tenue à Jérusalem du 27 au 29 octobre 2010.

([48]) Avis 8/2010 du groupe de travail «Article 29» sur le droit applicable, WP 179.

([49]) Sur les transferts internationaux, voir aussi le chapitre 8 du présent avis.

— établissant des procédures de coopération pour l'adoption de ces règles, y compris des critères pour la sélection d'une autorité de supervision principale (guichet unique).

9. **Le secteur de la police et de la justice**

9.1. *L'instrument général*

128. La Commission a maintes fois souligné l'importance de renforcer la protection des données dans le contexte de l'application du droit et de la prévention de la criminalité, où l'échange et l'utilisation de données à caractère personnel se sont considérablement intensifiés. En outre, le programme de Stockholm, approuvé par le Conseil européen, mentionne comme principal prérequis à l'application de la stratégie européenne de gestion de l'information dans ce domaine, l'instauration d'un régime efficace de protection des données ([50]).

129. La révision du cadre général de la protection des données est l'occasion idéale de progresser en la matière, en particulier si l'on se réfère au fait que la communication décrit à juste titre la décision-cadre 2008/977 comme étant inadéquate ([51]).

130. Le CEPD a expliqué, dans la section 3.2.5 du présent avis, les raisons pour lesquelles le domaine de la coopération policière et judiciaire devrait être inclus dans l'instrument général. Cette inclusion offre plusieurs avantages supplémentaires. Cela signifie que les règles ne s'appliqueront plus uniquement aux échanges de données transfrontières ([52]), mais aussi aux traitements nationaux. Cela permet également de garantir plus efficacement une protection adéquate en cas d'échange de données à caractère personnel avec des pays tiers, notamment dans le cadre d'accords internationaux. En outre, les autorités chargées de la protection des données disposeront des mêmes pouvoirs étendus et harmonisés à l'égard de la police et des autorités judiciaires que ceux dont ils jouissent à l'heure actuelle à l'égard des autres responsables du traitement. Enfin, l'actuel article 13, qui habilite les États membres à adopter des législations spécifiques pour restreindre les obligations et les droits établis par l'instrument général dans des intérêts publics spécifiques, devra s'appliquer de manière aussi restrictive qu'il est appliqué dans les autres domaines. En particulier, les garanties spécifiques prévues dans l'instrument général devront être également respectées dans la législation nationale adoptée dans le domaine de la coopération policière et judiciaire.

9.2. *Des règles spécifiques supplémentaires pour la police et la justice*

131. Toutefois, cette inclusion n'exclut pas les règles et dérogations spéciales, qui prennent dûment en compte les spécificités de ce secteur, conformément à la déclaration 21 annexée au traité de Lisbonne. Des limitations des droits des personnes concernées sont envisageables, mais elles doivent être nécessaires, proportionnées et ne pas altérer les éléments essentiels du droit lui-même. Il est à noter dans ce contexte que la directive 95/46/CE, y compris son article 13, s'applique à l'heure actuelle à l'application du droit dans divers domaines (p. ex. la fiscalité, les douanes, la lutte antifraude) qui ne diffèrent pas fondamentalement de nombreuses activités dans le domaine de la police et de la justice.

132. En outre, des garanties spécifiques doivent également être mises en place en vue de dédommager la personne concernée en lui accordant une protection supplémentaire dans un domaine où le traitement de données à caractère personnel risque d'être plus intrusif.

133. Sur la base de ce qui précède, le CEPD estime que le nouveau cadre devrait inclure au moins les éléments suivants, conformément à la convention 108 et à la recommandation n° R (87) 15:

— une distinction entre les différentes catégories de données et de fichiers en fonction de leur degré de précision et de leur fiabilité, sur la base du principe selon lequel il convient de distinguer les données reposant sur des faits des données reposant sur des avis ou une évaluation personnelle;

— une distinction entre les différentes catégories de personnes concernées (suspects, victimes, témoins, etc.) et de fichiers (temporaires, permanents, confidentiels). Il convient de prévoir des conditions et des garanties spécifiques pour le traitement des données concernant des personnes autres que les suspects;

— des mécanismes de vérification et de rectification périodiques afin de garantir la qualité des données traitées;

— des dispositions et/ou garanties spécifiques peuvent être instaurées en rapport avec le traitement (de plus en plus justifié) de données biométriques et génétiques dans le domaine de l'application du droit. Leur utilisation devrait être limitée exclusivement aux cas dans lesquels aucun moyen moins intrusif produisant le même effet n'est disponible ([53]);

— les modalités de transfert de données à caractère personnel à des autorités non compétentes et à des parties privées, ainsi que les modalités d'accès et d'utilisation ultérieure, par les forces répressives, de données à caractère personnel collectées par des parties privées.

([50]) Voir à cet égard l'avis du Contrôleur européen de la protection des données du 30 septembre 2010 sur la communication de la Commission au Parlement européen et au Conseil — «Présentation générale de la gestion de l'information dans le domaine de la liberté, de la sécurité et de la justice», paragraphes 9-19.

([51]) Voir la section 3.2.5 ci-dessus.

([52]) Il s'agit à l'heure actuelle du champ d'application limité de la décision-cadre 2008/977.

([53]) À cet égard, voir le document du groupe de travail sur l'avenir de la protection de la vie privée, point 112.

9.3. *Les régimes sectoriels de protection des données*

134. La communication prévoit ce qui suit: «la décision-cadre ne remplace pas les divers instruments législatifs de nature sectorielle qui ont été adoptés au niveau de l'Union dans les domaines de la coopération policière et judiciaire en matière pénale, notamment ceux qui régissent le fonctionnement d'Europol, d'Eurojust, du système d'information Schengen (SIS) et du système d'information des douanes (SID), qui prévoient des régimes particuliers de protection des données et/ou généralement renvoient à des instruments de protection des données du Conseil de l'Europe».

135. Le CEPD estime qu'un nouveau cadre juridique devrait, dans la mesure du possible, être clair, simple et cohérent. Si Europol, Eurojust, SIS et Prüm, par exemple, appliquent des régimes différents, le respect des règles reste compliqué, quand il ne se complique pas encore davantage. C'est l'une des raisons pour lesquelles le CEPD se prononce en faveur d'un instrument juridique général applicable à tous les secteurs.

136. Toutefois, le CEPD est conscient que l'harmonisation des règles issues de différents systèmes nécessitera un travail considérable, qu'il convient de mener à bien consciencieusement. Selon lui, une approche progressive, telle que mentionnée dans la communication, est valable pour autant que la volonté de garantir un niveau élevé de protection des données de manière cohérente et efficace reste claire et visible. Plus concrètement:

— dans un premier temps, l'instrument juridique général pour la protection des données devrait s'appliquer à tous les traitements dans le domaine de la coopération policière et judiciaire, y compris les ajustements introduits pour la police et la justice (tels qu'entendus dans la section 9.2);

— dans un deuxième temps, les régimes sectoriels de protection des données devraient être mis en conformité avec cet instrument général. La Commission devrait s'engager à adopter, à court terme et à une date déterminée, des propositions pour cette deuxième phase.

10. **Les autorités chargées de la protection des données et la coopération entre celles-ci**

10.1. *Renforcer le rôle des autorités chargées de la protection des données*

137. Le CEPD soutient pleinement l'objectif de la Commission de trancher la question du statut des autorités chargées de la protection des données (APD), et plus explicitement de renforcer leur indépendance, leurs ressources et leurs pouvoirs en matière de mise en œuvre de la législation.

138. Le CEPD insiste par ailleurs sur la nécessité de clarifier, dans le nouvel instrument juridique, la notion essentielle d'indépendance des APD. La Cour de justice européenne s'est récemment prononcée sur ce point dans l'affaire C-518/07 ([54]), dans laquelle elle a souligné que l'indépendance signifiait l'absence de toute influence extérieure. Une APD ne peut ni solliciter ni suivre l'avis de quiconque. Le CEPD suggère explicitement de codifier ces éléments d'indépendance dans un acte législatif.

139. Afin de pouvoir remplir leurs missions, les APD doivent disposer de ressources humaines et financières suffisantes. Le CEPD suggère d'inclure cette exigence dans la législation. ([55]) Il souligne finalement la nécessité de veiller à ce que les compétences des autorités en matière d'enquête et d'application de mesures de réparation et de sanctions suffisamment dissuasives soient totalement harmonisées, afin d'améliorer la sécurité juridique pour les personnes concernées et les responsables du traitement.

140. Le renforcement de l'indépendance, des ressources et des compétences des APD devrait aller de pair avec un renforcement de la coopération au niveau multilatéral, en particulier eu égard au nombre croissant de problèmes rencontrés en matière de protection des données à l'échelle européenne. Il apparaît clairement que la principale infrastructure adaptée pour la mise en œuvre de cette coopération est le groupe de travail «Article 29».

10.2. *Renforcer le rôle du groupe de travail*

141. Il est apparu au fil du temps que depuis ses débuts en 1997, le fonctionnement du groupe a évolué. Celui-ci a gagné en indépendance et ne peut plus être considéré, dans la pratique, comme un simple groupe de travail consultatif au sein de la Commission. Le CEPD suggère de continuer à améliorer le fonctionnement du groupe de travail, notamment son infrastructure et son indépendance.

142. Le CEPD est convaincu que la force du groupe réside fondamentalement dans l'indépendance et les prérogatives de ses membres. Son autonomie doit être préservée dans le nouveau cadre juridique, conformément aux critères établis pour une indépendance totale des APD par la Cour de justice européenne dans l'affaire C-518/07. Le CEPD estime que le groupe devrait aussi être doté de ressources et d'un budget suffisants ainsi que d'un secrétariat renforcé, afin de soutenir ses contributions.

143. Concernant le secrétariat du groupe de travail, le CEPD estime judicieux de l'avoir intégré dans l'unité sur la protection des données de la DG Justice, ce qui permet au groupe lui-même de bénéficier de contacts efficaces et flexibles et d'informations actualisées sur les dernières évolutions en matière de protection des données. En revanche, il conteste le fait que la Commission (et plus spécifiquement l'unité) soit à la fois membre, secrétariat et destinataire des avis du groupe de travail. Cela justifierait une indépendance accrue du secrétariat. Le CEPD encourage la Commission à évaluer — en étroite concertation avec les parties prenantes — le moyen de garantir au mieux cette indépendance.

([54]) Affaire C-518/07, *Commission/Allemagne*, non encore publiée au Recueil.

([55]) Voir, par exemple, l'article 43, paragraphe 2, du règlement (CE) n° 45/2001, qui prévoit une telle exigence pour le CEPD.

144. Enfin, le renforcement des pouvoirs des APD requiert aussi un renforcement des pouvoirs du groupe de travail, à l'aide d'une structure incluant de meilleures règles et garanties et garantissant une transparence accrue. Il concernera aussi bien le rôle consultatif que le rôle coercitif du groupe.

10.3. *Le rôle consultatif du groupe de travail*

145. Les avis du groupe de travail doivent être mis en œuvre de manière effective s'agissant de son rôle consultatif auprès de la Commission, en particulier en ce qui concerne l'interprétation et l'application des principes de la directive et des autres instruments en matière de protection des données. En d'autres termes, il convient de garantir le caractère officiel des positions du groupe. Les débats doivent se poursuivre au sein des APD afin de déterminer les moyens d'inclure cet aspect dans l'instrument juridique.

146. Le CEPD recommande diverses solutions pour donner plus de poids aux avis du groupe de travail sans pour autant modifier substantiellement son mode de fonctionnement. Il suggère d'inclure une obligation, pour les APD et la Commission, de tenir le plus grand compte des avis et positions communes adoptés par le groupe de travail, sur la base du modèle adopté pour les positions de l'Organe des régulateurs européens des communications électroniques (ORECE) ([56]). En outre, le nouvel instrument juridique pourrait confier au groupe la mission explicite d'adopter des «recommandations interprétatives». Ces solutions alternatives confèreraient aux positions du groupe un rôle accru, également devant les tribunaux.

10.4. *Une mise en œuvre coordonnée de la législation assurée par le groupe de travail*

147. Dans le cadre actuel, le contrôle de la mise en œuvre de la législation sur la protection des données dans les États membres est assuré par les vingt-sept autorités chargées de la protection des données, avec peu de coordination concernant le traitement de certains cas. Dans les cas impliquant plus d'un État membre ou ayant une dimension résolument mondiale, ce manque de coordination multiplie les coûts pour les entreprises, qui sont contraintes de traiter avec plusieurs administrations pour une même activité, et accroît le risque d'application incohérente: dans certains cas exceptionnels, un même traitement peut être jugé licite par une APD et illicite par une autre.

148. Certaines affaires comportent une dimension stratégique qu'il convient d'examiner de manière centralisée. Le groupe de travail «Article 29» facilite la coordination et l'adoption de mesures coercitives entre les APD ([57]) dans des affaires majeures ayant trait à la protection des données et ayant des implications internationales, telles que celles concernant des réseaux sociaux et des moteurs de recherche ([58]), ou des inspections coordonnées menées dans différents États membres au sujet de questions relatives aux télécommunications et à l'assurance maladie.

149. Le cadre actuel impose cependant des limites au groupe de travail concernant l'adoption de mesures de contrôle de la mise en œuvre de la législation. Des positions communes peuvent être adoptées, mais aucun instrument ne garantit l'application effective de ces positions dans la pratique.

150. Le CEPD suggère d'inclure dans l'instrument juridique de nouvelles dispositions à l'appui d'une mise en œuvre coordonnée, en particulier:

— une obligation de s'assurer que les APD et la Commission tiennent le plus grand compte des avis et positions communes du groupe ([59]);

— une obligation pour les APD de coopérer de bonne foi entre elles ainsi qu'avec la Commission et le groupe de travail ([60]). À titre d'exemple de coopération de bonne foi, il pourrait être envisagé de mettre en place une procédure par laquelle les APD informeraient la Commission ou le groupe de travail en cas d'adoption de mesures de mise en œuvre nationales comportant une dimension transfrontière, de manière analogue avec la procédure applicable dans le cadre actuel en rapport avec des décisions d'alignement nationales;

— préciser les règles de vote afin d'inciter davantage les APD à exécuter les décisions du groupe de travail. Il pourrait être établi que le groupe de travail envisage de prendre ses décisions sur la base d'un consensus et qu'en l'absence de consensus, il ne les prend qu'à la majorité qualifiée. Un considérant pourrait aussi prévoir qu'en émettant un vote positif sur un

([56]) Règlement (CE) nº 1211/2009 du Parlement européen et du Conseil du 25 novembre 2009 instituant l'Organe des régulateurs européens des communications électroniques (ORECE) ainsi que l'Office, (JO L 337 du 18.12.2009, p. 1).

([57]) Outre le groupe de travail «Article 29», la conférence européenne des commissaires à la protection des données a créé, il y a une dizaine d'années, un atelier permanent chargé de traiter les plaintes transfrontières de manière coordonnée. Bien que cet atelier présente une valeur ajoutée indéniable en termes d'échanges entre les membres des personnels des APD et fournisse un réseau fiable de points de contact, il ne peut être considéré comme un mécanisme de coordination des processus décisionnels.

([58]) Voir les lettres du groupe de travail du 12 mai 2010 et du 26 mai 2010, publiées sur le site du groupe (http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/2010-others_en.htm).

([59]) Comme indiqué plus haut, une obligation similaire est prévue dans le règlement (CE) nº 1211/2009, qui précise le rôle de l'Organe des régulateurs européens des communications électroniques (ORECE).

([60]) Voir, à cet égard, l'article 3 du règlement (CE) nº 1211/2009, précité.

document, les APD contractent une obligation ou un engagement en vue de sa mise en œuvre au niveau national.

151. Le CEPD met en garde contre l'introduction de mesures plus fermes, comme donner une force contraignante aux positions du groupe de travail, par exemple. Cela compromettrait l'indépendance de chaque APD, qui doit être garantie par les États membres en vertu du droit national. Si les décisions du groupe avaient une incidence directe sur des tiers tels que les responsables du traitement, de nouvelles procédures devraient être envisagées, dont des garanties comme la transparence ou la réparation, y compris éventuellement un recours devant la Cour de justice européenne.

10.5. *La coopération entre le CEPD et le groupe de travail*

152. Les modalités de coopération entre le CEPD et le groupe de travail pourraient aussi être affinées. Le CEPD est membre du groupe et contribue au sein de ce dernier à l'élaboration des positions sur les principaux développements stratégiques au sein de l'UE, tout en maintenant une cohérence dans ses propres positions. Il constate un nombre croissant de problèmes en matière de respect de la vie privée, tant dans le secteur privé que dans le secteur public, qui ont des répercussions au niveau national dans de nombreux États membres, et où le groupe de travail peut jouer un rôle spécifique.

153. Le CEPD a également pour tâche d'émettre des avis sur les développements qui ont lieu dans le cadre de l'UE, laquelle devrait être maintenue. En tant qu'organe européen, il exerce cette compétence consultative à l'égard des institutions de l'UE de la même manière que les APD nationales conseillent leurs gouvernements.

154. L'angle d'action du CEPD et celui du groupe de travail sont différents mais complémentaires. Il est donc nécessaire de préserver, voire d'améliorer la coordination entre ces deux entités, afin de s'assurer qu'elles collaborent sur les principales questions en matière de protection des données, par exemple en coordonnant leurs programmes de travail à intervalles réguliers ([61]) et en garantissant la transparence sur des questions comportant une dimension européenne spécifique ou plus nationale.

155. La coordination n'est pas mentionnée dans la directive actuelle pour la simple et bonne raison que le CEPD n'existait pas au moment de son adoption. Cependant, après six ans d'existence, les complémentarités du CEPD et du groupe de travail sont visibles et pourraient être officiellement reconnues. Le CEPD rappelle qu'en vertu du règlement (CE) nº 45/2001, il a le devoir de coopérer avec les APD nationales et de participer aux activités du groupe de travail. Il recommande de mentionner explicitement la coopération dans le nouvel instrument juridique et de la structurer si nécessaire, par exemple en établissant une procédure de coopération.

10.6. *La coopération entre le CEPD et les APD dans le domaine de la supervision des systèmes de l'UE*

156. Ces considérations s'appliquent aussi aux domaines dans lesquels il convient de coordonner la supervision entre le niveau européen et le niveau national. Tel est le cas lorsque des organes de l'UE traitent de grandes quantités de données fournies par les autorités nationales, ou dans le cadre de systèmes d'information à grande échelle dotés d'une composante nationale et d'une composante européenne.

157. Le système existant applicable à certains organes de l'UE et à certains vastes systèmes d'information européens à grande échelle — par exemple, Europol, Eurojust et le système d'information Schengen (SIS) première génération ont des organes de supervision conjoints comptant des représentants des APD nationales — est un vestige de la coopération intergouvernementale avant Lisbonne, qui ne respecte pas la structure institutionnelle de l'UE dont Europol et Eurojust font aujourd'hui partie intégrante, et dans laquelle l'acquis Schengen est à présent intégré ([62]).

158. La communication annonce que la Commission lancera en 2011 une consultation des parties prenantes au sujet de la révision de ces systèmes de supervision. Le CEPD prie instamment la Commission de prendre position dans les plus brefs délais (à court terme et à une date déterminée, voir ci-dessus) dans la discussion en cours concernant la supervision. Sa propre position se définit comme suit.

159. Dans un premier temps, il conviendrait de garantir que tous les organes de supervision remplissent les critères indispensables d'indépendance, de ressources et de pouvoirs de mise en œuvre de la législation. En outre, il conviendrait de s'assurer que les perspectives et l'expertise qui existent au niveau de l'UE sont prises en compte. En d'autres termes, une coopération devrait être établie non seulement entre les autorités nationales mais également avec l'APD européenne (actuellement le CEPD). Le CEPD estime qu'il est nécessaire de suivre un modèle qui respecte ces exigences ([63]).

160. On a assisté ces dernières années au développement du modèle de «supervision coordonnée». Ce modèle, d'ores et déjà opérationnel dans Eurodac et dans certaines parties du système d'information douanier, sera prochainement étendu au système d'information sur les visas (VIS) ainsi qu'au système d'information Schengen deuxième génération (SIS II). Il comporte trois couches: 1) la supervision

([61]) Par exemple sur la base de l'inventaire des activités législatives publiées annuellement et mises à jour régulièrement, qui est disponible sur le site du CEPD.

([62]) En vertu du règlement (CE) nº 45/2001, le CEPD est tenu de coopérer avec ces organes.

([63]) Pour Eurojust, un modèle devrait également prendre en compte le fait que la supervision de la protection des données doit respecter l'indépendance des magistrats, dans la mesure où Eurojust traite des données dans le cadre de procédures pénales.

au niveau national est assurée par les APD; 2) la supervision au niveau européen est assurée par le CEPD; 3) la coordination est assurée au moyen de réunions régulières convoquées par le CEPD agissant en qualité de secrétariat de ce mécanisme de coordination. Ce modèle s'est avéré efficace et a produit d'excellents résultats. Son utilisation devrait être envisagée à l'avenir pour d'autres systèmes d'information.

C. **COMMENT AMÉLIORER L'APPLICATION DU CADRE ACTUEL?**

11. **Le court terme**

161. Alors que le processus de révision est en cours, des efforts devraient être consacrés à garantir une application totale et effective des règles en vigueur. Ces règles resteront applicables jusqu'à l'adoption du futur cadre et sa transposition dans le droit national des différents États membres. Dans ce sens, plusieurs lignes d'action peuvent être mises en évidence.

162. En premier lieu, il conviendrait que la Commission continue de vérifier que les États membres se conforment à la directive 95/46/CE et, si nécessaire, use de ses pouvoirs en vertu de l'article 258 TFUE. Récemment, des procédures en infraction ont été engagées pour défaut d'application correcte de l'article 28 de la directive concernant l'exigence d'indépendance des APD ([64]). Dans d'autres domaines pareillement, il convient de vérifier et de garantir la pleine conformité ([65]). Le CEPD salue et soutient sans réserve l'engagement de la Commission à poursuivre une politique active de répression des infractions. Elle devrait aussi poursuivre le dialogue structurel engagé avec les États membres concernant la mise en œuvre ([66]).

163. Deuxièmement, les mesures de contrôle de la mise en œuvre au plan national doivent être encouragées afin de garantir une application concrète des règles en matière de protection des données, également en ce qui concerne les nouveaux phénomènes technologiques et les acteurs globaux. Les APD devraient user pleinement de leurs pouvoirs d'enquête et d'application de sanctions. Il importe par ailleurs que les droits existants des personnes concernées, en particulier le droit d'accès, soient pleinement respectés dans la pratique.

164. Troisièmement, une coordination accrue des mesures de mise en œuvre de la législation semble nécessaire à court terme. Le rôle du groupe de travail «Article 29» et de ses documents interprétatifs à cet égard est crucial, mais les APD devraient aussi faire tout ce qui est en leur pouvoir pour les mettre en pratique. Il importe d'éviter les issues divergentes dans les affaires à dimension européenne ou mondiale; des approches communes peuvent et doivent être adoptées au sein du groupe de travail. Des enquêtes coordonnées dans toute l'Union, menées sous les auspices du groupe, peuvent aussi s'avérer particulièrement utiles.

165. Quatrièmement, les principes de protection des données devraient être «intégrés» à titre préventif dans de nouvelles réglementations susceptibles d'avoir un impact, directement ou indirectement, sur la protection des données. A l'échelle de l'UE, le CEPD déploie des efforts considérables pour contribuer à la mise en place d'une meilleure législation européenne; pareils efforts doivent également être consentis au niveau national. Les APD devraient par conséquent exercer pleinement leurs pouvoirs consultatifs aux fins de cette approche préventive. Elles peuvent aussi — CEPD compris — jouer un rôle préventif en surveillant les évolutions technologiques. Cette surveillance est importante pour détecter à un stade précoce les tendances émergentes et cerner ainsi les implications possibles pour la protection des données, soutenir la mise en place de solutions respectueuses de la vie privée et sensibiliser les parties prenantes.

166. En dernier lieu, il importe de promouvoir activement une coopération plus étroite entre les divers acteurs au niveau international. À cette fin, les instruments internationaux de coopération doivent être renforcés. Des initiatives telles que les normes de Madrid et les travaux en cours au sein du Conseil de l'Europe et de l'OCDE méritent d'être pleinement soutenues. Dans ce contexte, il est particulièrement réjouissant de constater que la Commission fédérale du commerce des États-Unis a rejoint la famille des commissaires à la protection des données et de la vie privée dans le cadre de leur conférence internationale.

D. **CONCLUSIONS**

OBSERVATIONS GÉNÉRALES

167. Le CEPD approuve dans l'ensemble la communication de la Commission, persuadé que la révision du cadre juridique actuel pour la protection des données est nécessaire pour garantir une protection efficace dans une société de l'information en constant développement et de plus en plus mondialisée.

168. La communication identifie les principaux problèmes et défis. Le CEPD partage l'avis de la Commission selon lequel un solide système de protection des données restera nécessaire à l'avenir, étant admis que les principes généraux existants de protection des données restent valables dans une société en profonde mutation. Il estime aussi, comme indiqué dans la communication, que les défis sont de taille et souligne que les solutions proposées devraient par conséquent être proportionnellement ambitieuses et améliorer l'efficacité de la protection. Il appelle donc à une approche plus ambitieuse sur un certain nombre de points.

169. Le CEPD est favorable sans réserve à l'approche globale de la protection des données. Il déplore cependant que la communication exclue certains domaines, tels que le traitement de données par les institutions et organes de l'UE,

([64]) Voir l'affaire C-518/07, précitée, et le communiqué de presse de la Commission du 28 octobre 2010 (IP/10/1430).

([65]) La Commission a engagé une procédure en infraction à l'encontre du Royaume-Uni pour violation présumée de diverses dispositions en matière de protection des données, dont l'exigence de confidentialité pour les communications électroniques dans le cadre de la publicité comportementale. Voir le communiqué de presse de la Commission du 9 avril 2009 (IP/09/570).

([66]) Voir le premier rapport de la Commission sur la mise en œuvre de la directive sur la protection des données, précité, p. 22 et suivantes.

de l'instrument juridique général. Si la Commission décidait de ne pas inclure ces domaines, le CEPD l'invite instamment à adopter une proposition au niveau européen aussi rapidement que possible, de préférence au plus tard fin 2011.

LES PRINCIPALES PERSPECTIVES

170. Pour le CEPD, les points de départ de la révision sont les suivants:

— les dispositions en matière de protection des données doivent autant que possible servir activement, plutôt qu'entraver, d'autres intérêts légitimes (tels que l'économie européenne, la sécurité des personnes et la responsabilité des gouvernements);

— les principes généraux de protection des données ne doivent ni ne peuvent être modifiés;

— la poursuite de l'harmonisation devrait être un objectif essentiel de la révision;

— la perspective des droits fondamentaux devrait figurer au cœur du processus. Un droit fondamental a pour but de protéger les citoyens en toutes circonstances;

— le nouvel instrument juridique doit inclure le secteur de la police et de la justice;

— le nouvel instrument juridique doit être formulé autant que possible dans un environnement technologique neutre et viser à créer une sécurité juridique à long terme.

LES ÉLÉMENTS D'UN NOUVEAU CADRE

Harmonisation et simplification

171. Le CEPD salue la volonté de la Commission d'étudier les moyens de garantir une harmonisation accrue de la protection des données au niveau européen. Il détermine les domaines dans lesquels une harmonisation améliorée et renforcée est urgente: définitions, motifs de traitement des données, droits des personnes concernées, transferts internationaux et autorités chargées de la protection des données.

172. Le CEPD suggère d'envisager les options suivantes pour simplifier et/ou réduire la portée des obligations de notification:

— limiter l'obligation de notification à certains types spécifiques de traitements comportant certains risques spécifiques;

— imposer une obligation d'enregistrement simple requérant l'enregistrement des responsables du traitement (au lieu d'exiger le long processus d'enregistrement de l'ensemble des traitements de données);

— introduire un formulaire standard de notification paneuropéen.

173. Selon le CEPD, un règlement, un instrument unique directement applicable dans les États membres, est le meilleur moyen de protéger le droit fondamental à la protection des données et de parvenir à une meilleure convergence au sein du marché intérieur.

Renforcer les droits des personnes

174. Le CEPD soutient la proposition de la communication de renforcer les droits des personnes. Il formule les suggestions suivantes:

— un principe de transparence pourrait être inclus dans la législation. Il est toutefois plus important de renforcer les dispositions existantes ayant trait à la transparence (p. ex. les articles 10 et 11 de la directive 95/46/CE);

— une disposition sur la notification des violations des données à caractère personnel (brèches de sécurité), qui étend l'obligation incluse dans la directive révisée «vie privée et communications électroniques» à l'ensemble des responsables du traitement, devrait être introduite dans l'instrument général;

— les limites du consentement devraient être définies plus précisément. Il devrait être envisagé d'élargir le champ des situations requérant un consentement exprès et d'adopter des règles supplémentaires pour l'environnement en ligne;

— de nouveaux droits devraient être introduits, tels que la portabilité des données et le droit à l'oubli, en particulier pour les services en ligne de la société de l'information;

— les intérêts des enfants devraient être mieux protégés grâce à de nouvelles dispositions, portant spécifiquement sur la collecte et le traitement ultérieur de leurs données;

— des mécanismes de recours collectif pour violation des règles en matière de protection des données devraient être introduits dans la législation de l'UE, dans le but d'habiliter des entités qualifiées à engager des poursuites au nom de groupes de personnes.

Renforcer les obligations des responsables de traitement

175. Le nouveau cadre doit contenir des mesures incitant les responsables du traitement à inclure à titre préventif des mesures de protection des données dans leurs processus opérationnels. Le CEPD propose l'introduction de dispositions générales sur la responsabilité («accountability») et la prise en compte du principe de respect de la vie privée dès la conception («privacy by design»). Une disposition sur les systèmes de certification du respect de la vie privée devrait également être introduite.

La mondialisation et le droit applicable

176. Le CEPD salue les efforts ambitieux déployés à ce stade dans le cadre de la conférence internationale des commissaires à la protection des données pour concevoir les «normes de Madrid», dans l'optique de les intégrer dans un instrument contraignant et d'organiser éventuellement une conférence intergouvernementale. Il invite la Commission à prendre des mesures concrètes en ce sens en étroite collaboration avec l'OCDE et le Conseil de l'Europe.

177. Un nouvel instrument juridique doit préciser les critères qui déterminent le droit applicable. Il convient de s'assurer que les données traitées dans des pays tiers n'échappent pas à la juridiction de l'UE lorsqu'il existe une demande justifiée d'appliquer le droit de l'UE. Si le cadre juridique prenait la forme d'un règlement, des règles identiques s'appliqueraient dans tous les États membres, ce qui réduirait la nécessité de déterminer le droit applicable (au sein de l'UE).

178. Le CEPD soutient pleinement l'objectif visant à garantir une approche plus uniforme et plus cohérente vis-à-vis des pays tiers et des organisations internationales. Des règles d'entreprise contraignantes devraient être incluses dans l'instrument juridique.

Le secteur de la police et de la justice

179. Un instrument général englobant le secteur de la police et de la justice pourrait autoriser l'inclusion de règles spéciales, qui prennent dûment en compte les spécificités de ce secteur, conformément à la déclaration 21 annexée au traité de Lisbonne. Des garanties spécifiques doivent être mises en place afin d'offrir une compensation aux personnes concernées en leur assurant une protection supplémentaire dans un domaine où le traitement de données à caractère personnel est par essence plus intrusif.

180. Le nouveau cadre juridique devrait, dans la mesure du possible, être clair, simple et cohérent. Il faut éviter qu'Europol, Eurojust, SIS et Prüm, par exemple, appliquent des régimes différents. Le CEPD est d'avis que le rapprochement des règles issues des différents systèmes devra se faire avec précaution et de manière progressive.

Les APD et la coopération entre les APD

181. Le CEPD soutient pleinement l'objectif de la Commission de trancher la question du statut des autorités chargées de la protection des données (APD), et plus explicitement de renforcer leur indépendance, leurs ressources et leurs pouvoirs de mise en œuvre de la législation. Il recommande:

— de codifier, dans le nouvel instrument juridique, la notion essentielle d'indépendance des APD, telle que définie par la CJUE;

— de prévoir dans la législation que les APD doivent disposer de ressources suffisantes;

— d'attribuer aux autorités des pouvoirs d'enquête et d'application de sanctions harmonisés.

182. Le CEPD suggère de nouvelles améliorations concernant le fonctionnement du groupe de travail «Article 29», notamment son indépendance et son infrastructure. Le groupe de travail devrait par ailleurs disposer de ressources suffisantes et d'un secrétariat renforcé.

183. Le CEPD suggère de renforcer le rôle consultatif du groupe en introduisant une obligation, pour les APD et la Commission, de *tenir le plus grand compte des avis et positions communes* adoptés par le groupe. Il pense préférable de ne pas donner une force contraignante aux positions du groupe, en particulier du fait du statut indépendant de chaque APD. Il recommande l'introduction par la Commission de dispositions spécifiques visant à améliorer la coopération avec le CEPD dans le nouvel instrument juridique.

184. Le CEPD prie instamment la Commission de se positionner aussi rapidement que possible sur la question de la supervision des organes de l'UE et de systèmes d'informations européens à grande échelle, à la lumière du fait que tous les organes de supervision doivent remplir les critères indispensables d'indépendance, de ressources suffisantes et de pouvoirs de mise en œuvre de la législation et qu'il convient de s'assurer que la perspective européenne est correctement représentée. Le CEPD soutient le modèle de «supervision coordonnée».

Améliorations dans le cadre du système actuel:

185. Le CEPD encourage la Commission à:

— continuer de vérifier que les États membres se conforment à la directive 95/46/CE et, si nécessaire, user de ses pouvoirs en vertu de l'article 258 TFUE;

— promouvoir la mise en œuvre de la législation au niveau national et sa coordination;

— intégrer à titre préventif des principes de protection des données dans de nouvelles réglementations susceptibles d'avoir une incidence, directement ou indirectement, sur la protection des données;

— promouvoir activement une coopération plus étroite entre les divers acteurs au niveau international.

Fait à Bruxelles, le 14 janvier 2011.

Peter HUSTINX

Contrôleur européen de la protection des données