Groupe de travail «Article 29» sur la protection des données

00062/10/FR
WP 173

Avis n° 3/2010 sur le principe de la responsabilité

Adopté le 13 juillet 2010

NOTE DE SYNTHÈSE

Il est fréquent que les principes et obligations à respecter dans l'Union européenne en matière de protection des données ne se traduisent pas suffisamment par des mesures et pratiques internes concrètes. À moins d'une réelle intégration dans les valeurs et pratiques communes d'une organisation et d'une répartition explicite des responsabilités, le respect de ces principes et obligations risque d'être compromis, et les incidents relatifs à la protection des données sont susceptibles de se perpétuer.

Pour favoriser la protection effective des données, le cadre réglementaire européen doit se doter d'outils complémentaires. Le présent avis a pour but de conseiller la Commission sur la manière de modifier la directive sur la protection des données dans ce sens. À cet égard, le présent avis formule une proposition concrète en vue d'établir un principe de responsabilité exigeant des responsables du traitement des données qu'ils mettent en place des mesures appropriées et efficaces pour garantir le respect des principes et obligations définis dans la directive, et qu'ils le prouvent aux autorités de contrôle qui le demandent. Cela contribuerait à faire de la protection des données une réalité et aiderait les autorités compétentes en la matière dans leurs missions de supervision et de mise en application.

L'avis contient en outre des suggestions visant à garantir que le principe de responsabilité offre la sécurité juridique requise, tout en laissant une certaine marge de manœuvre aux acteurs de la protection (par exemple, en leur permettant de déterminer les mesures concrètes à mettre en place selon les risques liés au traitement et les types de données traités). Il examine ensuite l'impact que pourrait avoir un tel principe sur d'autres domaines, dont les transferts de données internationaux, les exigences en matière de notification, les sanctions et, enfin, il aborde l'élaboration de programmes de certification ou de labels.

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

créé par la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995,

vu les articles 29 et 30, paragraphe 1, point a, et paragraphe 3, de ladite directive, et l'article 15, paragraphe 3, de la directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002,

vu son règlement intérieur,

a adopté l'avis suivant.

1. INTRODUCTION

1. La protection des données doit devenir une réalité. Les prescriptions légales en la matière doivent se traduire par de véritables mesures de protection des données. Pour favoriser la protection effective des données, le cadre juridique européen en la matière doit se doter de mécanismes complémentaires. Au cours des discussions sur l'avenir du cadre européen et mondial de protection des données, il a été suggéré de recourir à des mécanismes reposant sur la responsabilité afin d'encourager les responsables du traitement des données à utiliser des outils pratiques en vue de garantir la protection effective des données.

2. Dans son document de décembre 2009 intitulé «L'avenir de la protection de la vie privée» (WP168), le groupe article 29 estimait que le cadre juridique actuel n'avait pas été pleinement en mesure de garantir la transposition des exigences en matière de protection des données en mécanismes efficaces offrant une réelle protection. Pour remédier à cette situation, le groupe proposait à la Commission d'envisager la mise en place de mécanismes basés sur le principe de responsabilité, en mettant tout particulièrement l'accent sur la possibilité d'intégrer un principe de responsabilité dans la version révisée de la directive relative à la protection des données[1]. Ce principe renforcerait le rôle du responsable du traitement des données et accroîtrait sa responsabilité.

[1] «Pour résoudre ce problème, il conviendrait d'introduire un principe de responsabilité dans le cadre global aux termes duquel les responsables du traitement des données seraient contraints de prendre les mesures nécessaires pour veiller au respect des obligations et principes essentiels de la directive actuelle lors du traitement des données à caractère personnel. Une telle disposition renforcerait la nécessité de mettre en place des politiques et des mécanismes permettant la mise en œuvre effective des principes et obligations essentiels de la directive actuelle. Elle confirmerait la nécessité de prendre des mesures efficaces donnant lieu à une application interne efficace des obligations et principes essentiels actuellement consacrés dans la directive. En outre, le principe de responsabilité exigerait des responsables du traitement des données qu'ils mettent en place les mécanismes internes nécessaires pour démontrer leur conformité aux parties prenantes externes, notamment aux autorités nationales chargées de la protection des données. Au final, la nécessité de prouver que les mesures appropriées ont été prises pour assurer la conformité facilitera considérablement l'exécution des règles applicables.» (WP168, point 79. Pour obtenir de plus amples informations, voir aussi les points 74 à 78).

3. Pour faire bref, disons qu'un principe légal de responsabilité exigerait expressément des responsables du traitement des données qu'ils mettent en œuvre des mesures appropriées et efficaces en vue de garantir le respect des principes et obligations prévus par la directive, et qu'ils soient en mesure d'en faire la preuve sur demande. En pratique, ceci se traduirait par des programmes évolutifs visant à appliquer les principes relatifs à la protection des données en vigueur (parfois appelés «programmes de conformité»). En complément de ce principe, d'autres exigences particulières, destinées à donner effet aux garanties en matière de protection des données ou à s'assurer de leur efficacité, pourraient être définies. On pourrait par exemple imaginer une disposition requérant la réalisation d'une évaluation de l'impact sur la vie privée pour toutes les opérations de traitement des données à plus haut risque.

4. Cet avis entend se fonder sur les contributions antérieures du groupe article 29 à ce sujet, formulées dans son avis sur l'avenir de la protection de la vie privée, en vue de conseiller la Commission dans le cadre de son actuel processus de révision de la directive 95/46/CE. Pour ce faire, le présent avis est divisé en quatre sections. La première aborde la nécessité, pour les responsables du traitement des données, de renforcer leurs dispositifs internes (politiques et procédures) en vue de s'assurer que toutes les opérations de traitement s'effectuent dans le respect des règles en vigueur et de voir comment des systèmes basés sur la responsabilité pourraient contribuer à cet objectif. Elle examine ensuite la forme que pourrait revêtir l'architecture juridique d'un système basé sur la responsabilité, ainsi que les précédents dans le domaine de la protection des données et dans d'autres domaines. La deuxième section avance une proposition concrète de principe de responsabilité et expose le raisonnement qui sous-tend les différents aspects de cette proposition. La troisième section traite des différents éléments liés à un système juridique, et notamment à un système général de responsabilité. Elle expose aussi la nécessité d'une telle proposition en vue de garantir la sécurité juridique, cette proposition étant cependant formulée dans des termes suffisamment larges de façon à laisser une certaine marge de manœuvre aux acteurs de la protection (ce qui permettrait de déterminer des mesures et méthodes de vérification concrètes à appliquer selon les risques liés au traitement et les types de données traités). Enfin, l'avis aborde d'autres questions connexes, telles que la relation avec les transferts internationaux; il décrit les avantages d'un mécanisme basé sur la responsabilité pour les autorités chargées de la protection des données et envisage le rôle éventuel de la certification dans ce contexte.

II. RESPONSABILITÉ: BUTS, ARCHITECTURE JURIDIQUE, PRÉCÉDENTS ET TERMINOLOGIE

II.1 La responsabilité comme moteur de l'application efficace des principes de protection des données

5. À l'heure actuelle, la nécessité et l'intérêt, pour les responsables du traitement des données, de garantir la mise en place de mesures efficaces assurant une réelle protection des données, se font de plus en plus sentir. Il y a à cela plusieurs raisons, que nous examinerons ci-après.

6. Tout d’abord, nous assistons à un véritable «déluge de données», avec une croissance continue du nombre de données à caractère personnel générées, traitées et transférées. Ce phénomène est favorisé tant par l’évolution technologique, à savoir la multiplication des systèmes d’information et de communication, que par la capacité grandissante des personnes à utiliser les technologies et à interagir avec celles-ci. À mesure que les volumes de données disponibles et circulant de par le monde augmentent, les risques pour leur confidentialité s'accroissent eux aussi. Ceci souligne encore la nécessité, pour les responsables du traitement des données, tant du secteur public que du secteur privé, de mettre en œuvre de véritables mécanismes internes efficaces en vue de garantir la protection des informations à caractère personnel.

7. Ensuite, cette croissance constante du volume d’informations à caractère personnel va de pair avec une augmentation de leur valeur sur le plan social, politique et économique. Dans certains secteurs, et surtout dans les environnements en ligne, les données à caractère personnel sont *de facto* devenues une monnaie d’échange pour les contenus en ligne. Dans le même temps, du point de vue sociétal, on reconnaît de plus en plus la valeur sociale de la protection des données. En bref, à mesure que les informations à caractère personnel gagnent en importance pour les responsables du traitement des données tous secteurs confondus, les citoyens, les consommateurs et la société dans son ensemble sont eux aussi de plus en plus conscients de leur valeur, ce qui renforce encore la nécessité d’appliquer des mesures strictes en vue de les préserver.

8. Enfin, il découle de ce qui précède que les divulgations de données à caractère personnel peuvent avoir un impact négatif majeur pour les responsables du traitement des données des secteurs public et privé. Tout incident potentiel lié à des applications d’administration ou de santé en ligne aurait des conséquences désastreuses sur le plan économique, mais surtout en termes de réputation. Il est par conséquent devenu capital pour les responsables du traitement des données de tous les secteurs de réduire les risques au minimum, de jouir d’une bonne réputation et de la conserver et de s’assurer la confiance des citoyens et des consommateurs.

9. En résumé, les points ci-dessus montrent qu’il est absolument nécessaire pour les responsables du traitement des données de mettre en œuvre des mesures de protection des données efficaces, visant une bonne gouvernance en la matière, tout en réduisant au minimum les risques juridiques et économiques ainsi que les risques d'atteinte à la réputation susceptibles de résulter de mauvaises pratiques en matière de protection des données. Comme nous le verrons plus en détail ci-après, c’est précisément le but des mécanismes fondés sur la responsabilité.

II.2 Une possible architecture juridique globale pour les mécanismes basés sur la responsabilité

10. Dans ce contexte, il est intéressant de s’interroger sur la manière dont le cadre juridique pourrait encourager les responsables du traitement des données à prendre des mesures offrant une réelle protection - en d’autres termes, de se demander à quoi devrait ressembler l’architecture juridique d’un système basé sur la responsabilité.

11. Avant d'entrer dans le vif du sujet, il convient de souligner d'emblée que ces systèmes ne modifieront et n'affecteront en rien les principes essentiels de la protection des données. Au contraire, ils ont pour but d'en améliorer l'application.

12. Une façon d'inciter les responsables du traitement des données à mettre en place de telles mesures serait d'insérer un principe de responsabilité dans la version révisée de la directive. Parmi les effets attendus d'une telle disposition figurent la mise en œuvre de mesures et procédures internes en vue d'appliquer les principes existants de protection des données et de garantir leur efficacité, ainsi que l'obligation de le démontrer à la demande des autorités chargées de la protection des données. Comme nous le verrons ci-après, le type de procédures et de mécanismes varierait selon les risques que posent le traitement et la nature des données.

13. En outre, on pourrait également envisager des exigences spécifiques, telles que l'obligation d'évaluer l'impact sur la vie privée dans certains cas ou la désignation de délégués à la protection des données personnelles. Ces prescriptions particulières pourraient venir compléter le principe général de responsabilité.

14. Le groupe de travail «article 29» reconnaît que les responsables du traitement des données pourraient vouloir mettre en œuvre des politiques et procédures qui ne soient pas expressément prévues par la législation relative à la protection des données. Par exemple, il se peut qu'un tel responsable veuille s'engager à répondre aux demandes d'accès dans des délais très brefs, alors que la législation prévoit une certaine souplesse, ou à répondre aux demandes d'accès simultanément en ligne et hors ligne, afin de garantir la bonne réception des informations dans un délai bref. On pourrait aussi imaginer une situation dans laquelle le responsable du traitement des données souhaiterait aller au-delà des exigences minimales prévues par le cadre juridique général. Il pourrait ainsi décider de désigner un délégué à la protection des données, bien que la législation en vigueur ne l'y contraigne pas, ou vouloir commander à une tierce partie un audit de *toutes* ses opérations de traitement des données afin d'évaluer si celles-ci sont conformes au cadre juridique relatif à la protection des données. Le groupe de travail «article 29» salue ces initiatives et souhaiterait que le nouveau cadre juridique relatif à la protection des données encourage les responsables du traitement des données à prendre de telles mesures.

15. Dans le droit fil de ce qui précède, l'«architecture juridique» des mécanismes de responsabilité prévoirait deux niveaux: le premier niveau consisterait en une exigence légale fondamentale contraignante pour *tous* les responsables du traitement des données, laquelle comprendrait deux éléments de fond: la mise en œuvre de mesures/procédures et la conservation d'une trace documentaire de celle-ci. Des exigences particulières pourraient venir compléter ce premier niveau. Le second niveau couvrirait des systèmes de responsabilité volontaires allant au-delà des exigences juridiques minimales, eu égard aux principes sous-jacents de la protection des données (offrir des garanties supérieures à celles requises par les règles en vigueur) et/ou en termes de modalités de mise en œuvre ou de contrôle de l'efficacité des mesures (définir des exigences plus strictes). Tout en reconnaissant l'importance et les avantages de tels systèmes, le présent avis

traitera principalement du premier niveau, et plus particulièrement du principe général de responsabilité.

II.3 Principe de responsabilité en matière de protection des données ainsi que dans d'autres domaines, et terminologie

Précédents

16. Le groupe de travail «article 29» tient à observer que le principe de responsabilité n'est pas neuf en soi. Sa reconnaissance explicite figure déjà dans les lignes directrices de l'Organisation de coopération et de développement économiques (OCDE) régissant la protection de la vie privée, adoptées en 1980. Sous «Principe de la responsabilité», celles-ci disposent: «*Tout maître de fichier devrait être responsable du respect des mesures donnant effet aux principes [matériels] énoncés ci-dessous*».

17. Dernièrement, ce principe a été explicitement inclus dans les «normes internationales de Madrid», élaborées par la Conférence internationale des commissaires à la protection des données et de la vie privée[2]. Il figure aussi dans la dernière version du projet de norme ISO 29100 établissant un cadre pour le respect de la vie privée et est l'un des principaux concepts du cadre de l'OCEAP (Organisation de coopération économique Asie-Pacifique) pour la protection de la vie privée et de ses règles transnationales en la matière[3].

18. D'un point de vue réglementaire, le groupe de travail «article 29» note que les principes énoncés dans la norme du Canada intitulée Code type sur la protection des renseignements personnels, annexés à la loi sur la protection des renseignements personnels et les documents électroniques, font référence à la responsabilité. Le premier principe, entre autres, exige l'élaboration et la mise en œuvre de politiques et de pratiques visant à respecter les dix principes énoncés dans ladite norme, et notamment la mise en œuvre de procédures pour protéger les renseignements à caractère personnel et la mise en place des procédures pour recevoir les plaintes et les demandes de renseignements et y donner suite.

19. Le groupe de travail «article 29» note par ailleurs que les règles d'entreprise contraignantes («BCR») appliquées dans le contexte des transferts de données internationaux prennent en compte le principe de responsabilité. En effet, ces règles constituent des codes de bonnes pratiques, élaborés et mis en œuvre par des organisations multinationales, qui contiennent des mesures internes visant à mettre en application les principes de la protection des données (telles des audits, des programmes de formation, un réseau de délégués à la protection de la vie privée, un système de gestion des plaintes). Une fois révisées par les autorités nationales

---

2 La personne responsable doit: «a) prendre les mesures nécessaires pour observer les principes et obligations exposés dans le présent document et dans la législation nationale applicable, et b) avoir les mécanismes internes en place pour démontrer l'observation des principes aux personnes concernées et aux autorités de contrôle dans l'exercice de leurs pouvoirs, comme prévu à l'article 23.»

3 Outre ce qui précède, le «Centre for Information Policy Leadership» participe actuellement à une initiative visant à explorer les effets du principe de responsabilité en matière de protection des données et de la vie privée. Voir www.informationpolicycentre.com

chargées de la protection des données, les BCR sont réputées offrir des garanties adéquates pour les transferts ou catégories de transferts de données à caractère personnel entre entreprises qui appartiennent au même groupe et sont liées par lesdites règles en vertu des articles 25 et 26, paragraphe 2, de la directive 95/46/CE.

20. En dehors du domaine de la protection des données, il existe aussi des exemples d'application du principe de responsabilité, comme un programme précisant les politiques et procédures des responsables du traitement des données en vue de garantir la conformité avec la législation et la réglementation en vigueur. La réglementation en matière de services financiers rend par exemple obligatoire le recours à des programmes de conformité. Dans d'autres secteurs, les programmes de conformité ne sont pas obligatoires mais sont encouragés, comme c'est le cas dans le droit de la concurrence. Ainsi, au Canada, le Bureau de la concurrence a-t-il élaboré des politiques très détaillées en matière de programmes de conformité d'entreprise, programmes auxquels les entreprises peuvent décider d'adhérer ou non sur base volontaire. Le Commissaire canadien de la concurrence souligne toutefois l'importance de la conformité en tant qu'outil d'atténuation des risques et met en avant ses avantages juridiques, économiques et en matière d'image.[4]

Terminologie

21. En anglais, on utilise le terme «accountability», issu du monde anglo-saxon où il est d'usage courant et où il existe un vaste consensus sur le sens à lui donner – bien qu'il soit difficile d'en définir avec précision le sens dans la pratique. Globalement, on peut toutefois dire qu'il met l'accent sur la manière dont la responsabilité (responsability) est assumée et sur la manière de le vérifier. En anglais, les termes «responsibility» et «accountability» sont comme l'avers et le revers d'une médaille et sont tous deux des éléments essentiels de la bonne gouvernance. On ne peut inspirer une confiance suffisante que s'il est démontré que la responsabilité (responsability) est efficacement assumée dans la pratique.

22. Dans la plupart des autres langues européennes, du fait, essentiellement, de la diversité des systèmes juridiques, il est difficile de traduire le terme «accountability». Il existe dès lors un risque réel d'interprétation différente du terme et, donc, d'absence d'harmonisation. D'autres termes ont été suggérés pour rendre le sens d'«accountability». Parmi ceux-ci: «reinforced responsibility» (responsabilité renforcée), «assurance», «reliability» (fiabilité), «trustworthiness» (crédibilité) et, en français, «obligation de rendre des comptes», etc. On peut aussi avancer que l'«accountability» renvoie à la «mise en œuvre des principes de protection des données».

23. Aux fins du présent document, nous avons choisi de nous concentrer sur les mesures à prendre ou à prévoir afin d'assurer la conformité dans le domaine de la protection des données. C'est dans ce sens qu'il faut entendre le terme de «responsabilité» utilisé dans le présent avis pour faire référence à l'anglais «accountability», sans préjudice de toute autre formule qui refléterait avec plus de précision le concept visé ici. C'est pourquoi le présent document ne se focalisera

4 http://www.bureaudelaconcurrence.gc.ca/eic/site/cb-bc.nsf/fra/02732.html.

pas sur les termes, mais, de manière plus pragmatique, sur les mesures à prendre, plutôt que sur le concept lui-même.

III. VERS UNE PROPOSITION DE DISPOSITION GÉNÉRALE EN MATIÈRE DE RESPONSABILITÉ

III.1 Une disposition générale visant à réaffirmer et à renforcer la responsabilité des responsables du traitement des données

24. Le groupe de travail «article 29» a réfléchi plus avant à la possibilité d'introduire, à la lumière des considérations évoquées à la section I, des solutions reposant sur la responsabilité dans le nouveau cadre juridique global en matière de protection des données.

25. Cette réflexion l'a conforté dans son opinion, déjà exprimée dans l'avis sur l'avenir de la protection de la vie privée, selon laquelle un principe général de responsabilité devrait être inclus dans un nouveau cadre législatif complet. L'objet d'une telle disposition consisterait à réaffirmer et à renforcer la responsabilité des responsables du traitement des données dans le cadre de leur mission, sans préjudice des éventuelles mesures concrètes venant compléter ce principe.

26. Cette nouvelle disposition s'inscrirait dans le droit fil de certaines dispositions déjà présentes dans le cadre législatif actuel. Citons, à cet égard et à titre d'exemple, l'article 6 de la directive 95/46/CE, qui fait référence, au paragraphe 1, aux principes relatifs à la qualité des données et mentionne, au paragraphe 2, qu'«il incombe au responsable du traitement d'assurer le respect du paragraphe 1». Ou encore l'article 17, paragraphe 1, qui exige des responsables du traitement des données qu'ils mettent en œuvre des mesures techniques et d'organisation. Une disposition générale de responsabilité renforcerait même la nécessité pour les responsables du traitement des données de respecter les exigences de l'article 17 en matière de sécurité, en plus des autres prescriptions.

III.2 Vers une proposition concrète de principe général de responsabilité

27. La nouvelle disposition viserait à favoriser l'adoption de mesures concrètes et pratiques, de manière à traduire les principes généraux de protection des données dans des politiques et procédures concrètes définies au niveau du responsable du traitement des données, conformément à la législation et à la réglementation en vigueur. Le responsable du traitement des données devrait également veiller à l'efficacité des mesures prises et pouvoir démontrer, sur demande, qu'il les a bien mises en œuvre.

28. De manière schématique, une telle disposition générale se concentrerait sur deux éléments centraux:

    (i) la nécessité pour le responsable du traitement des données de prendre des mesures appropriées et efficaces pour mettre en œuvre les principes de protection des données;

(ii) la nécessité de démontrer, sur demande, que des mesures appropriées et efficaces ont été prises. En conséquence, le responsable devrait fournir des preuves de l'exécution du point (i) ci-dessus.

29. Cette obligation devrait s'appliquer à tous les responsables du traitement des données, en toutes circonstances.

30. Le premier élément de l'obligation exigerait des responsables du traitement des données qu'ils mettent en œuvre des mesures appropriées. Les types de mesures visés ne seraient pas précisés dans le texte de la disposition générale, mais des orientations ultérieures, émises par les autorités nationales chargées de la protection des données, par le groupe de travail «article 29» ou par la Commission (via les procédures de comitologie) pourraient spécifier, pour certains cas, un ensemble minimal de mesures spécifiques jugées appropriées. Citons, à titre d'exemple, l'adoption, dans certaines circonstances, des politiques et procédures internes nécessaires à la mise en œuvre des principes de protection des données, qui refléteraient la législation et la réglementation en vigueur.

31. La mise en œuvre de ces mesures et procédures pourrait aussi se faire efficacement par l'attribution de responsabilités et la formation des agents participant aux opérations de traitement des données. Ainsi, les responsables du traitement des données devraient-ils notamment être encouragés à désigner des délégués à la protection des données à caractère personnelle, conformément à l'article 18 de la directive. Il convient, en tout état de cause, d'encourager l'attribution de responsabilités à différents niveaux de l'organisation, en vue de garantir que celles-ci sont bien assumées.

32. Concernant les transferts de données à caractère personnel à destination de pays tiers, les responsables du traitement des données devraient adopter et mettre en œuvre des mesures appropriées pour se conformer à l'exigence, prévue à l'article 26 de la directive, d'offrir des «garanties suffisantes» telles que les BCR.

33. Les responsables du traitement des données doivent également s'assurer que les mesures pratiques mises en œuvre en vue d'observer les principes de protection des données sont efficaces. Dans le cas d'opérations de traitement de données de plus grande ampleur, plus complexes ou à haut risque, l'efficacité des mesures adoptées devrait faire l'objet d'un contrôle régulier. Il existe différentes manières d'évaluer l'efficacité (ou l'inefficacité) des mesures: contrôles, audits internes et externes, etc.

34. À la lumière des remarques exposées ci-dessus, le groupe de travail «article 29» s'est penché sur le libellé d'une proposition concrète qui pourrait être introduite dans un cadre législatif global. Celle-ci pourrait être formulée comme suit:

«Article X – Mise en œuvre des principes de protection des données»

1. Le responsable du traitement prend des mesures efficaces et appropriées en vue de garantir le respect des principes et obligations énoncés dans la directive.
2 À la demande de l'autorité de contrôle, le responsable du traitement apporte à celle-ci la preuve du respect des dispositions du paragraphe 1.

IV. EXAMEN DE DIVERS ÉLÉMENTS LIÉS AU PRINCIPE GÉNÉRAL DE RESPONSABILITÉ

IV.1 Renforcement des obligations existantes

35. Le groupe de travail «article 29» note que certains responsables du traitement des données pourraient percevoir le principe général de responsabilité comme une source de nouvelles exigences légales lourdes pour eux, surtout compte tenu de la situation économique difficile que connaît actuellement l'Union européenne. Ce serait une erreur.

36. Le groupe de travail «article 29» tient à souligner que la plupart des exigences énoncées dans cette nouvelle disposition existent en fait déjà dans la législation en vigueur, bien qu'elles y soient moins explicites. En vertu du cadre juridique actuel, les responsables du traitement des données sont d'ores et déjà tenus, en effet, de se conformer aux principes et obligations qui figurent dans la directive. Pour ce faire, il est intrinsèquement nécessaire de mettre en place des procédures liées à la protection des données et d'éventuellement les vérifier. De ce point de vue, une disposition relative à la responsabilité ne constitue pas une grande nouveauté et, pour l'essentiel, n'impose pas d'exigences qui n'existent déjà implicitement dans la législation en vigueur. Globalement, la nouvelle disposition ne vise pas à soumettre les responsables du traitement des données à de nouveaux principes, mais plutôt à assurer le respect *de facto* des principes existants.

37. En fait, une évolution législative analogue a eu lieu en 2009, lorsque la directive 2002/58/CE a été modifiée[5]. Dans ce cas, la législation impose la mise en œuvre d'une politique de sécurité, et ce afin d'«[assurer] *la mise en œuvre d'une politique de sécurité relative au traitement des données à caractère personnel*». S'agissant des dispositions de ladite directive en matière de sécurité, le législateur a donc décidé qu'il était nécessaire d'introduire une exigence explicite d'élaboration et de mise en place d'une politique de sécurité. Par ailleurs, l'article 18 de la directive 95/46/CE, qui fait référence à la désignation d'un détaché à la protection des données, de même que le système des règles d'entreprise contraignantes mentionné ci-dessus, offrent déjà des exemples de mesures pratiques qui peuvent être adoptées par les responsables du traitement des données.

38. Autre question en relation avec le point ci-dessus: les conséquences de la conformité (ou de la non-conformité) au principe de responsabilité. Le groupe de travail «article 29» tient à signaler que le fait d'observer le principe de responsabilité ne signifie pas pour autant qu'un responsable du traitement des données soit en conformité avec les principes matériels énoncés dans la directive.

---

5 Directive 2009/136/CE du Parlement européen et du Conseil du 25 novembre 2009 modifiant la directive 2002/22/CE concernant le service universel et les droits des utilisateurs au regard des réseaux et services de communications électroniques, directive 2002/58/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques et règlement (CE) n° 2006/2004 relatif à la coopération entre les autorités nationales chargées de veiller à l'application de la législation en matière de protection des consommateurs.

En d'autres termes, ce principe n'offre aucune présomption juridique de conformité et ne remplace aucun desdits principes. Un responsable du traitement des données peut avoir mis en œuvre et vérifié les mesures mises en place et néanmoins être en défaut. Par conséquent, l'adoption, par un responsable du traitement des données, de mesures destinées à observer les principes ne doit en aucun cas exclure la mise en œuvre à son encontre de mesures coercitives lorsque les autorités chargées de la protection des données l'estiment nécessaire. En pratique, toutefois, les responsables du traitement des données des secteurs public et privé qui ont adopté des mesures dans le cadre de programmes de conformité solides sont plus susceptibles d'être en conformité avec la législation. En effet, ayant mis en place des mesures efficaces destinées à observer les principes matériels de la protection des données, il est moins vraisemblable qu'ils enfreignent la législation. Par conséquent, lors de l'évaluation des sanctions relatives aux violations des principes de protection des données, les autorités chargées de la protection des données devraient tenir compte de la mise en œuvre (ou de l'absence de mise en œuvre) de mesures et de leur vérification.

IV.2 Mesures appropriées en vue de mettre en œuvre les dispositions de la directive

39. Une disposition relative à la responsabilité exigerait des responsables du traitement des données qu'ils définissent et mettent en œuvre les mesures requises pour garantir la conformité de leurs opérations avec les principes et obligations de la directive et en fassent vérifier l'efficacité de manière périodique.

40. Le principe général de responsabilité qui est proposé évite à dessein de trop détailler les types de mesures à prendre. Ceci soulève les deux questions fondamentales et connexes suivantes: *i)* Quelles sont les mesures courantes qui assureraient le respect du principe de responsabilité? *ii)* Comment proportionner et adapter les mesures à des circonstances spécifiques?

Les mesures: illustration

41. Le groupe de travail «article 29» considère que les mesures de responsabilité courantes pourraient inclure la liste – non exhaustive – suivante:

- instauration de procédures internes *avant* la création de nouvelles opérations de traitement de données à caractère personnel (contrôle interne, évaluation, etc.);[6]
- mise en place de politiques de protection des données écrites et contraignantes, à prendre en compte et à appliquer aux nouvelles opérations de traitement des données (par exemple, conformité aux critères de qualité des données, préavis, principes de sécurité, consultation, etc.), lesquelles devraient être mises à la disposition des personnes concernées;
- mappage des procédures en vue de veiller au bon recensement de toutes les opérations de traitement des données et gestion d'un inventaire de celles-ci;

[6] Les opérations de traitement des données existantes devraient bénéficier d'une période de transition en vue de leur mise en conformité avec la législation.

- désignation d'un délégué à la protection des données et d'autres personnes responsables de la protection des données;
- mise en place d'une protection des données adéquate et d'une formation pour les agents. Parmi ceux-ci, citons les personnes chargées (ou responsables) du traitement des données à caractère personnel (directeurs des ressources humaines, par exemple), mais aussi les directeurs informatiques, développeurs et directeurs d'entités opérationnelles. Des ressources suffisantes doivent être mises à disposition pour la gestion de la protection de la vie privée;
- mise en place de procédures de gestion des demandes d'accès, de rectification et d'effacement, qui doivent être transparentes pour les personnes concernées;
- mise sur pied d'un mécanisme interne de gestion des plaintes;
- élaboration de procédures internes pour une gestion et une déclaration efficaces des infractions;
- réalisation d'évaluations d'impact sur la vie privée dans certaines circonstances;
- mise en œuvre et supervision de procédures de vérification afin de s'assurer que toutes les mesures n'existent pas seulement sur papier, mais qu'elles sont aussi mises en œuvre et fonctionnent dans la pratique (audits internes ou externes, etc.).

42. Une stratégie complémentaire au principe général de responsabilité pourrait également être envisagée. Dans cette hypothèse, le cadre juridique pourrait non seulement inclure un principe de responsabilité général, mais aussi une liste indicative de mesures susceptibles d'être encouragées au niveau national[7]. Cette

---

[7] Par exemple, les normes internationales adoptées à Madrid par les autorités chargées de la protection des données prévoient, à l'article 22, une disposition relative aux mesures proactives, qui dit ceci: «*Les États, à travers leur législation nationale, pourront encourager la mise en œuvre, par ceux qui sont impliqués à un quelconque stade du traitement, de mesures visant à promouvoir une meilleure conformité aux lois applicables sur la protection de la vie privée en relation avec le traitement de données personnelles. De telles mesures pourraient inclure, entre autres:*

a) la mise en œuvre de procédures de prévention et de détection des manquements, qui pourraient être basées sur les modèles standardisés de gouvernance de sécurité de l'information et/ou de gestion de la sécurité de l'information;

b) la nomination d'un ou plusieurs correspondants à la protection des données, dotés des qualifications, ressources et pouvoirs suffisants pour exercer leur fonction de supervision de manière adéquate;

c) la réalisation périodique de programmes de formation, d'éducation, de sensibilisation auprès des membres des organisations pour une meilleure compréhension des lois applicables sur la protection de la vie privée en relation avec le traitement de données personnelles, ainsi que des procédures établies par les organisations à cet effet;

d) la réalisation périodique d'audits transparents, réalisés par des parties qualifiées et de préférence indépendantes afin de vérifier la conformité aux lois applicables sur la protection de la vie privée en relation avec le traitement de données personnelles, ainsi qu'aux procédures établies par les organisations à cet effet;

e) l'adaptation des systèmes et/ou technologies de l'information pour le traitement de données personnelles aux lois applicables sur la protection de la vie privée en relation avec le traitement de données personnelles, particulièrement au moment de décider de leurs spécifications techniques et de leur développement et mise en œuvre;

f) la mise en œuvre d'évaluations de l'impact sur la vie privée préalablement à la mise en œuvre de nouveaux systèmes et/ou technologies de l'information pour le traitement de données

disposition pourrait contenir une liste indicative et non exhaustive de mesures susceptibles de devenir la «boîte à outils» des responsables du traitement des données. Elle fournirait ainsi des orientations aux responsables sur ce qui pourrait constituer, selon les cas, les mesures appropriées à prendre. Cette liste ne ferait bien sûr qu'accompagner l'obligation légale générale d'adopter des mesures appropriées.

Proportionnalité des mesures

43. La liste ci-dessus est indicative des mesures que les responsables du traitement des données pourraient mettre sur pied pour assurer le respect de la première partie du principe de responsabilité («*Le responsable du traitement prend des mesures efficaces et appropriées pour garantir le respect des principes et obligations énoncés dans la directive.*»*)*

44. Certaines de ces mesures sont des «mesures fondamentales» qui devront être mises en œuvre dans la plupart des opérations de traitement des données. L'élaboration d'actions et de procédures internes visant l'application des principes (procédures de gestion des demandes d'accès, des plaintes) peut constituer un exemple de mesure appropriée pour certaines opérations de traitement. L'adéquation des mesures devra être établie au cas par cas. Il incombe aux responsables du traitement des données de prendre de telles décisions, sur la base des orientations émises par les autorités nationales chargées de la protection des données et par le groupe de travail «article 29», le cas échéant (voir ci-dessous).

45. Il découle de ce qui précède que, pour déterminer les types de mesures à mettre en œuvre, seules des options «sur mesure» sont possibles. En effet, les mesures spécifiques à appliquer doivent être arrêtées selon les faits et circonstances de chaque cas particulier, compte tenu, en particulier, du risque associé au traitement et aux types de données. Une stratégie unique aurait pour seul effet d'obliger les responsables du traitement des données à mettre en place des structures inadaptées et se solderait par un échec.

46. Dans cette optique, les responsables doivent être à même d'élaborer des mesures répondant aux spécificités de leur situation particulière et des opérations de traitement concernées. À cet égard, le groupe de travail «article 29» rappelle les critères utilisés à l'article 17 de la directive actuelle[8] pour déterminer le type de

---

personnelles, ainsi qu'avant la mise en place de nouvelles méthodes de traitement de données personnelles, ou de toutes modifications substantielles dans le traitement existant;

g) l'adoption de codes d'autorégulation contraignants, qui incluent des éléments permettant de mesurer leur efficacité en matière de conformité et de niveau de protection des données personnelles, et qui prévoient des mesures efficaces en cas de non-conformité;

h) la mise en œuvre d'un plan d'intervention établissant des lignes directrices d'action à prendre dans l'hypothèse d'un manquement aux lois applicables sur la protection de la vie privée en relation avec le traitement de données personnelles, incluant au moins l'obligation de déterminer la cause et l'étendue du manquement, de décrire ses effets dommageables et de prendre les mesures appropriées pour éviter qu'il ne se reproduise dans le futur.»

8 *«Ces mesures doivent assurer, compte tenu de l'état de l'art et des coûts liés à leur mise en œuvre, un niveau de sécurité approprié au regard des risques présentés par le traitement et de la nature des données à protéger.»*

mesures de sécurité à appliquer, à savoir les risques associés au traitement des données et à la nature de celles-ci. Ces deux facteurs peuvent être utilisés de manière analogue afin de déterminer les types généraux de mesures à appliquer. Plus concrètement, des aspects comme l'ampleur des opérations de traitement, les buts de celui-ci et le nombre de transferts de données envisagés peuvent contribuer à définir le niveau de risque. Le type de données, notamment leur éventuel caractère sensible, doit également être pris en compte. Une réflexion quant à la nécessité d'imposer certaines obligations aux sous-traitants de données ou aux concepteurs et/ou producteurs de TIC (technologies de l'information et de la communication) pourrait également être menée à la lumière de ce principe de responsabilité.

47. Tout en se conformant à ces critères, les grandes organisations responsables du traitement de données devraient, en principe, mettre en œuvre des mesures strictes. Dans certains cas, les organisations de taille modeste ou moyenne, par exemple si elles effectuent des opérations de traitement de données à risque, telles des données liées aux dossiers médicaux en ligne, peuvent également être tenues de mettre en place des garanties rigoureuses. Ainsi, une administration locale (municipalité), une multinationale, une petite entreprise en ligne, une organisation pour laquelle le traitement des données constitue une activité centrale ou une organisation avec des antécédents d'infractions auraient toutes besoin de mesures spécifiques pour assurer une gouvernance crédible et efficace des informations. Dès lors, dans des cas simples comme le traitement des données à caractère personnel liées aux ressources humaines en vue de créer un répertoire d'entreprise, il pourrait facilement être satisfait à l'«obligation de démontrer» à laquelle fait référence le paragraphe 2 de la disposition sur la responsabilité (par exemple, par la présentation des notes d'information utilisées, une description des mesures élémentaires de sécurité, etc.). En revanche, dans d'autres situations plus complexes, impliquant par exemple le recours à des dispositifs biométriques innovants, respecter l'«obligation de démontrer» pourrait exiger d'autres mesures. Il se peut ainsi que le responsable du traitement ait à démontrer qu'il a réalisé une évaluation de l'impact sur la vie privée, que les agents chargés du traitement ont été formés et qu'ils sont régulièrement informés, etc.

48. La transparence fait partie intégrante des nombreuses mesures de responsabilité. La transparence vis-à-vis des personnes concernées et du public en général contribue à une plus grande responsabilité des responsables du traitement des données. Ainsi, il est possible d'obtenir un degré de responsabilité supérieur en publiant les politiques de protection de la vie privée sur l'internet, en assurant la transparence quant aux procédures internes de gestion des plaintes et en publiant des rapports annuels.

Orientations et sécurité juridique

49. Si la nécessité d'une solution évolutive, et donc d'une certaine souplesse, justifie l'utilisation d'un langage transparent, le groupe de travail «article 29» est conscient qu'une disposition générale, flexible et offrant une marge d'adaptation peut aussi être source d'insécurité. Les responsables du traitement pourraient ainsi considérer que la disposition n'est pas suffisamment détaillée pour garantir la

sécurité juridique. Il se peut, par exemple, qu'ils ne soient pas sûrs du niveau de détail requis dans les politiques et procédures de respect de la vie privée, du moment et de la manière de désigner un délégué à la protection des données, du moment d'organiser des séances de formation, etc. Cette incertitude peut également porter sur le type de contrôle, externe ou interne, qui est nécessaire. Par ailleurs, les responsables du traitement des données pourraient aussi craindre de se voir imposer des interprétations nationales divergentes et arbitraires quant à la portée et à la nature de leurs obligations.

50. Le groupe de travail «article 29» comprend ces inquiétudes. Toutefois, pour les raisons exposées ci-dessus concernant la nécessité de prévoir une certaine souplesse et une certaine adaptabilité, il n'est pas possible d'inclure dans la directive elle-même une solution permettant de garantir la sécurité juridique. Pour parvenir à la sécurité juridique requise, le groupe de travail considère qu'il pourrait être utile d'harmoniser les orientations émises par la Commission (au moyen de mesures techniques de mise en œuvre, par exemple) et/ou par le groupe de travail «article 29», en vue d'offrir une plus grande sécurité et d'éliminer les éventuelles divergences au niveau de la mise en œuvre[9]. Le groupe de travail pourrait également préparer des orientations générales ébauchant les éléments nécessaires pour tout responsable du traitement des données quel qu'il soit. Cette base pourrait ensuite être adaptée aux besoins spécifiques de chaque responsable.

51. Il peut également être utile de développer un *modèle de programme de conformité des données*, qui servirait de base aux organisations de moyenne et de grande taille pour élaborer leur propre programme, comme cela a été fait pour les BCR, sur la base des orientations élaborées par le groupe de travail «article 29»[10]. Ces modèles devraient être créés après un examen minutieux des pratiques en cours et des modèles disponibles, et après consultation de toutes les parties prenantes concernées. Il s'agit là d'un domaine qui exigera un investissement important de tous les acteurs.

Efficacité des mesures

52. Les problèmes abordés ci-avant concernant les mesures à appliquer se posent également dans le contexte de la garantie de leur efficacité. Suivant le type de traitement de données, les moyens de garantir l'efficacité des mesures mises en place seront différents.

53. Les responsables du traitement des données peuvent évaluer l'efficacité (ou l'inefficacité) des mesures de différentes manières. Pour les opérations de grande envergure, complexes et à haut risque, il est fréquent d'avoir recours à des audits internes et externes. La manière dont les audits sont réalisés peut également varier,

---

9 Publié par le Commissariat à la protection de la vie privée du Canada, l'outil d'auto-évaluation LPRPDE est un exemple d'orientation de cette nature. Cet outil aide les organisations de moyenne et de grande taille à élaborer et à mettre en œuvre de bonnes pratiques de gouvernance et de gestion de la protection de la vie privée. Il est disponible à l'adresse: http://www.priv.gc.ca/information/pub/ar-vr/pipeda_sa_tool_200807_f.pdf.

10 Document de travail n° 153 du groupe de travail «article 29» établissant un tableau des éléments et principes à reprendre dans les règles d'entreprise contraignantes et document de travail n° 154 établissant un cadre pour la structure des règles d'entreprise contraignantes.

allant de l'audit complet à l'audit négatif (lesquels peuvent, à leur tour, revêtir différentes formes). Pour définir les modalités permettant de garantir l'efficacité des mesures, le groupe de travail «article 29» suggère d'appliquer les mêmes critères que ceux utilisés pour déterminer les mesures, lesquels découlent de l'article 17 de la directive 95/46/CE, à savoir les risques posés par le traitement des données et la nature de celles-ci. La manière dont un responsable garantira l'efficacité des mesures dépendra par conséquent du caractère sensible des données, des volumes de données traités et des risques particuliers associés aux opérations de traitement. Les orientations du groupe de travail «article 29» sur les mesures pourraient également inclure des orientations à ce sujet.

IV.3 Corrélation avec d'autres exigences

Notifications préalables

54. Une réflexion pourrait être menée quant à l'impact possible sur les notifications préalables d'une définition de garanties appropriées au niveau du responsable du traitement. On pourrait envisager que certains mécanismes de responsabilité remplacent ou réduisent les exigences administratives prévues par l'actuelle législation sur la protection des données, comme l'a déjà suggéré le groupe de travail «article 29» dans son avis sur l'avenir de la protection de la vie privée.

Transferts de données internationaux

55. Les règles d'entreprise contraignantes sont un exemple de la manière dont les principes de protection des données peuvent être mis en œuvre sur la base du principe de responsabilité. Elles constituent une manière reconnue et acceptée par le groupe de travail «article 29» de fournir des garanties adéquates pour les transferts à destination de pays tiers.
56. Il s'agit là d'un domaine qui gagnerait à être étudié plus avant à la lumière de la révision de la directive 95/46/CE. Il importe notamment d'examiner si, en vertu de l'article 26, paragraphe 2, de la directive («*un État membre peut autoriser un transfert [...] lorsque le responsable du traitement offre des garanties suffisantes [...]; ces garanties peuvent notamment résulter de clauses contractuelles appropriées»)*, les règles d'entreprise contraignantes et éventuellement d'autres mécanismes de responsabilité contraignants analogues sont réputés offrir des garanties suffisantes.

57. Dans ce contexte, il serait extrêmement intéressant d'évaluer, entre autres choses, les mécanismes utilisés en interne chez les responsables du traitement des données pour mettre en application les principes et obligations de protection des données, ainsi que leurs systèmes de vérification. Il serait également judicieux de débattre de mécanismes qui permettraient de rationaliser le système actuel reposant sur l'autorisation des transferts de données par les autorités nationales chargées de la protection des données.

IV.4 Le rôle des autorités chargées de la protection des données

58. Une question se pose néanmoins : le principe de responsabilité proposé dans le présent avis aura-t-il un impact sur les pouvoirs des autorités chargées de la protection des données, notamment dans le domaine de la mise en application? Comme expliqué ci-après, le principe ne privera les autorités chargées de la protection des données d'aucune de leurs prérogatives. Au contraire, il comportera des avantages pour elles.

59. En ce qui concerne l'exécution, le principe tel qu'il est proposé réaffirme la compétence des autorités chargées de la protection des données de demander au responsable du traitement des preuves de sa conformité au principe de responsabilité; il renforce donc les activités de surveillance desdites autorités. Ceci garantit que les autorités restent compétentes pour, à tout moment, prendre des mesures coercitives. Il convient de souligner que, en tout état de cause, les autorités chargées de la protection des données restent compétentes pour superviser non seulement les mesures prises par les responsables du traitement des données mais, surtout, la conformité aux principes et obligations sous-jacents.

60. Par ailleurs, mettre le principe de responsabilité en application permettra aux autorités chargées de la protection des données de disposer d'informations utiles pour surveiller le degré de conformité. En effet, puisque les responsables du traitement des données devraient être en mesure de démontrer aux autorités qu'ils ont mis en œuvre les mesures et de quelle manière, des informations très pertinentes en matière de conformité seraient dès lors à la disposition des autorités. Celles-ci pourraient alors utiliser ces informations aux fins de leur mission de surveillance. Par ailleurs, si ces informations ne leur étaient pas fournies sur demande, les autorités chargées de la protection des données auraient une raison immédiate d'agir à l'encontre des responsables, indépendamment de la violation présumée d'autres principes de protection des données sous-jacents.

61. Ce principe devrait également être déterminant pour les autorités chargées de la protection des données, en ce sens qu'il les aiderait à être plus sélectives et stratégiques, leur permettant d'investir leurs ressources de manière à générer la plus large conformité possible.

62. Le groupe de travail «article 29» note que le principe de responsabilité peut contribuer à l'émergence d'une expertise juridique et technique dans le domaine de la mise en œuvre des exigences en matière de protection des données. Des personnes disposant de solides connaissances, ainsi que d'une bonne compréhension des aspects techniques et juridiques de la protection des données, mais aussi d'excellentes aptitudes à la communication, à la formation du personnel, ainsi qu'à l'élaboration et à la mise en œuvre de politiques et d'audits seront indispensables dans ce domaine. Une telle expertise sera nécessaire tant en interne que sous la forme d'un service externe auquel les entreprises pourront avoir recours. Cette évolution sera capitale pour garantir que les responsables du traitement des données assument leurs obligations, au besoin en réalisant des audits internes et externes/internes. Dans le même temps, elle sera bénéfique pour les autorités de protection des données puisque, dans la mesure où le système contribuera à la conformité globale, les autorités auront à leur disposition

davantage d'informations solides sur les pratiques internes des entreprises, et l'apparition de professionnels de la protection des données hautement qualifiés et compétents facilitera sans aucun doute leur interaction avec les responsables du traitement des données.

63. On peut conclure que l'activité des autorités de protection des données est davantage centrée sur un rôle «ex post» qu'«ex ante». La responsabilité mettant l'accent sur certains résultats à obtenir en termes de bonne gouvernance de la protection des données, on considère qu'elle est orientée sur les résultats et met l'accent sur son rôle «ex post» (en d'autres termes, elle intervient après le début du traitement des données).

IV.5 Sanctions

64. Le système proposé ne peut fonctionner que si les autorités chargées de la protection des données sont dotées de compétences notables en matière de sanction. À cet égard, si et lorsque des responsables du traitement des données ne respectent pas le principe de responsabilité, il faut que des sanctions significatives puissent leur être imposées. Par exemple, un responsable du traitement des données qui n'honorerait pas les engagements qu'il a pris au titre des politiques internes contraignantes devrait pouvoir être sanctionné. Ceci vient bien sûr s'ajouter à la violation proprement dite des principes essentiels de la protection des données.

65. Outre ce qui précède, le groupe de travail «article 29» considère que les pouvoirs des autorités nationales chargées de la protection des données devraient inclure la possibilité d'imposer aux responsables du traitement des données des instructions précises concernant leurs systèmes de conformité.

IV.6 Développement de programmes de certification

66. À plus long terme, la disposition relative à la responsabilité pourrait favoriser la mise en place de programmes de certification ou de labels. De tels programmes contribueraient à prouver qu'un responsable du traitement des données a bien respecté la disposition, qu'il a défini et mis en œuvre des mesures appropriées et que celles-ci ont fait l'objet d'un audit périodique. Divers facteurs peuvent favoriser une telle évolution.

67. En règle générale, on peut s'attendre à ce que, pour se distinguer de la concurrence et créer un avantage concurrentiel, les services d'évaluation de l'impact sur la vie privée/d'audit/de protection des données proposent de plus en plus des certificats et labels. Les responsables du traitement des données pourront alors décider d'avoir recours à des services fiables qui délivrent des certificats. Lorsque certains labels seront connus pour leurs tests rigoureux, les responsables du traitement des données pourraient privilégier ceux-ci pour bénéficier d'un plus grand «confort» en matière de conformité, et pour se doter d'un avantage concurrentiel.

68. Si des BRC sont utilisées comme base juridique des transferts de données internationaux, les responsables du traitement des données sont tenus de démontrer qu'ils ont mis en place des garanties suffisantes, auquel cas les autorités chargées de la protection des données peuvent autoriser les transferts. Il s'agit également d'un domaine dans lequel des services de certification pourraient s'avérer utiles. De tels services analyseraient les garanties fournies par le responsable du traitement des données et, le cas échéant, les certifieraient. Les autorités chargées de la protection des données pourraient alors utiliser ces certificats délivrés au titre d'un programme de certification donné lorsqu'elles analysent les BCR pour savoir si un responsable du traitement des données a fourni des garanties suffisantes aux fins de transferts de données internationaux. Le processus d'autorisation de ce type de transferts en serait simplifié.

IV.7 Réglementation des programmes de certification

69. Les raisons qui justifient l'instauration de services de certification soulignent aussi la nécessité de réglementer ceux-ci. En effet, si ces services ont pour objet de fournir des preuves fiables de la conformité en matière de protection des données (aux autorités chargées de la protection des données, aux responsables du traitement et aux consommateurs en général) et qu'ils doivent s'intégrer sans heurts au marché intérieur, il semble nécessaire de définir des règles pour leur fourniture. Les autorités chargées de la protection des données devraient jouer un rôle clé dans l'élaboration de ces règles (par exemple, données de référence, modèles, etc.) et être en mesure de les faire appliquer, ce qui suppose qu'elles disposent aussi des ressources suffisantes à cet effet. Par ailleurs, les autorités chargées de la protection des données ont aussi un rôle à jouer dans la certification des organismes de certification, surtout dans le domaine des transferts de données internationaux. La qualité des services et la nécessité qu'ils respectent les règles du marché intérieur étant des critères clés, la législation devra établir les conditions permettant de parvenir à une telle qualité. Il ne semble pas possible de laisser faire le marché. L'expérience dans d'autres domaines, et notamment dans la certification des marchandises, a montré une tendance au nivellement par le bas. La concurrence entre prestataires pourrait conduire à une baisse des prix, ainsi qu'à une certaine souplesse, voire à un assouplissement, des procédures. Bref, qu'elles soient ou non arrêtées à l'échelon transfrontalier, des règles semblent nécessaires pour garantir la bonne qualité des services et des conditions égales pour tous.

70. Le groupe de travail «article 29» note que la législation en vigueur en matière d'accréditation[11] peut s'appliquer aux services de certification dans le domaine de la protection des données. Cette législation fournit déjà la structure nécessaire pour établir les règles en matière d'organisation et de fonctionnement des organismes d'accréditation. Ces règles s'appliquent à l'accréditation volontaire, ainsi que dans les cas spécifiques où une accréditation est obligatoire.

---

[11] Règlement (CE) n° 765/2008 du Parlement européen et du Conseil du 9 juillet 2008 fixant les prescriptions relatives à l'accréditation et à la surveillance du marché pour la commercialisation des produits et abrogeant le règlement (CEE) n° 339/93.

71. Il va de soi que ce type de services favoriserait aussi l'harmonisation des normes sous-jacentes sur la base desquelles les entités seraient évaluées. Les orientations mentionnées (émanant du groupe de travail «article 29» ou de la Commission), définissant des modèles de programmes de conformité des données, joueraient à cet égard un rôle de premier plan.

V. CONCLUSIONS

72. L'évolution des nouvelles technologies et la mondialisation de plus en plus marquée de l'économie et de la société ont conduit à une prolifération des informations à caractère personnel collectées, triées, transférées ou conservées à d'autres fins. Par conséquent, les risques associés à ces données se multiplient aussi.

73. Le groupe de travail «article 29» est convaincu que l'augmentation, tant des risques que de la valeur des données à caractère personnel, justifie en soi de renforcer le rôle et la responsabilité des responsables du traitement des données. Un cadre réglementaire tenant compte de cette nouvelle donne doit prévoir les outils nécessaires en vue d'encourager les responsables du traitement des données à mettre en pratique des mesures appropriées et efficaces assurant que les principes de protection des données portent leurs fruits. Des procédures visant à recenser toutes les opérations de traitement des données, à répondre aux demandes d'accès et à répartir les ressources judicieusement, notamment en désignant des personnes responsables de l'organisation de la conformité en matière de protection des données sont autant d'exemples de ces mesures.

74. Pour favoriser la protection des données dans la pratique, le groupe de travail «article 29» suggère tout d'abord d'inclure dans les propositions de modification de la directive relative à la protection des données une nouvelle disposition exigeant des responsables du traitement des données qu'ils mettent en œuvre des mesures appropriées et efficaces pour garantir le respect des principes et obligations en la matière, et qu'ils démontrent cette mise en conformité aux autorités qui le demandent. Ces mesures devraient favoriser la conformité aux principes et obligations en matière de protection des données tout en limitant les risques d'accès non autorisé, d'abus, de pertes, etc. L'obligation de démontrer, sur demande, la mise en place des mesures requises devrait, pour les autorités chargées de la protection des données, se révéler un instrument utile qui les aidera dans leur mission de surveillance.

75. L'obligation de mettre en œuvre ces mesures devrait s'appliquer aux responsables du traitement des données de tous les secteurs (privé et public) et être adaptable, de manière à ce que le type de mesures prises soit proportionné aux risques associés au traitement des données et à la nature de celles-ci.

Fait à Bruxelles, le 13 juillet 2010

Pour le groupe de travail,
le président,
Jacob KOHNSTAMM