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 européen et au Comité des régions intitulée «L'identification par radiofréquence (RFID) en Europe: vers un cadre politique», document COM(2007) 96

(2008/C 101/01)

LE CONTRÔLEUR EUROPÉEN DE LA PROTECTION DES DONNÉES,

vu le traité instituant la Communauté européenne, et notamment son article 286,

vu la Charte des droits fondamentaux de l'Union européenne, et notamment son article 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,

vu la directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques,

vu le règlement (CE) n° 45/2001 du Parlement européen et du Conseil du 18 décembre 2000 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données, et notamment son article 41,

A ADOPTÉ L'AVIS SUIVANT:

I. INTRODUCTION

1. Le 15 mars 2007, la Commission a adopté une communication intitulée «L'identification par radiofréquence (RFID) en Europe: vers un cadre politique» ([1]) (ci-après dénommée: «la communication»). En vertu de l'article 41 du règlement (CE) n° 45/2001, le CEPD est chargé de conseiller les institutions et organes communautaires et les personnes concernées pour toutes les questions concernant le traitement des données à caractère personnel. Le CEPD présente le présent avis conformément à cet article.

2. Le présent avis doit être considéré comme une réaction du CEPD à la communication de la Commission, ainsi qu'à d'autres mesures qui ont été prises dans le domaine de la RFID depuis l'adoption de la communication, à savoir:

   — la décision de la Commission du 28 juin 2007 instituant le groupe d'experts sur l'identification par radiofréquence ([2]), qui est une conséquence directe de la communication. Ce groupe est également connu en anglais sous le nom de «RFID — Stakeholders Group» (groupe des parties prenantes sur les RFID. Conformément à l'article 4, paragraphe 4, point b), de la décision, le CEPD participe aux travaux de ce groupe en qualité d'observateur,

   — la résolution du Conseil du 22 mars 2007 relative à une stratégie pour une société de l'information sûre en Europe ([3]),

   — le projet «RFID et gestion de l'identité», lancé par le Parlement européen ([4]),

([1]) COM(2007) 96 final.
([2]) Décision n° 467/2007/CE (JO L 176 du 6.7.2007, p. 25).
([3]) JO C 68 du 24.3.2007, p. 1.
([4]) Projet «RFID and identity management — Case studies from the frontline of the development towards ambient intelligence», realisé par le groupe eurropéen d'évaluation des technologies (ETAG), à la demande du service d'évaluation des choix technologiques et scientifiques (STOA) du Parlement européen http://www.europarl.europa.eu/stoa/default_en.htm

— l'avis nº 4/2007 sur le concept de données à caractère personnel adopté en juin 2007 par le Groupe de l'article 29 sur la protection des données) ([1]),

— la communication de la Commission au Parlement européen et au Conseil intitulée «Suivi du programme de travail pour une meilleure mise en application de la directive sur la protection des données» ([2]) et l'avis rendu par le CEPD sur cette communication en date du 25 juillet 2007 ([3]),

— la proposition de directive, adoptée par la Commission, modifiant (notamment) la 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 ([4]).

3. Le CEPD accueille favorablement la communication de la Commission sur la RFID, car elle aborde les principales questions qui se posent dans le cadre du déploiement des technologies RFID sans négliger celles — essentielles — qui ont trait à la protection de la vie privée et des données. Cette communication a bénéficié de travaux préparatoires méthodiques et rigoureux: cinq ateliers thématiques, ainsi qu'une consultation publique en ligne ([5]), réalisée à l'initiative de la Commission, l'ont en effet précédée.

4. Le CEPD reconnait que les systèmes RFID pourraient jouer un rôle crucial dans le développement de la société de l'information, phénomène généralement désigné sous le nom d'«internet des objets», et il partage pleinement les préoccupations exprimées au point 3.2 de la communication selon lesquelles les systèmes RFID risquent de porter atteinte aux droits à la vie privée des personnes et à la protection des données. Dans son rapport annuel 2005, il a d'ailleurs défini la technologie RFID, ainsi que l'utilisation de la biométrie, des environnements intelligents et des systèmes de gestion des identités, comme des développements technologiques susceptibles d'avoir des incidences majeures sur la protection des données.

5. Selon le CEPD, la domestication des technologies RFID et leur acceptation par le grand public ne seront pas seulement fonction de l'attrait que présentent la commodité et les nouveaux services offerts, mais elles seront aussi facilitées par les avantages que confèrent des systèmes de protection des données adaptés et cohérents.

6. En résumé, le CEPD qualifie la technologie RFID d'évolution technologique fondamentalement nouvelle, désignée à juste titre dans la communication de la Commission comme une passerelle vers une nouvelle phase de développement de la société de l'information.

7. Cette évolution suscite des questions importantes dans différents domaines, notamment dans celui de la protection des données et du respect de la vie privée — domaine auquel le présent avis du CEPD sera limité.

II. ÉLÉMENTS FONDAMENTAUX DE L'AVIS DU CEPD

8. Le présent avis porte en particulier sur les conséquences que cette évolution risque d'avoir sur la protection des données et le respect de la vie privée. Ces conséquences sont aujourd'hui incertaines, notamment du fait que la mise au point des systèmes RFID et leur domestication sont en pleine évolution et que personne ne peut prédire avec certitude quel en sera l'aboutissement.

9. C'est pourquoi le CEPD a adopté l'approche suivante:

— en premier lieu, il cherche à recenser les conséquences pratiques du déploiement des systèmes RFID sur la protection des données et le respect de la vie privée,

— en deuxième lieu, il s'attache à qualifier ces conséquences au regard du cadre juridique actuellement en place en matière de protection des données et de la vie privée,

— en troisième lieu, il s'interroge sur la nécessité éventuelle d'adopter des règles plus spécifiques afin de traiter les problèmes de protection des données suscités par l'utilisation des technologies RFID. Il a déjà soulevé cette question dans son avis sur la communication relative à la directive sur la protection des données et il l'examinera plus en détail dans le présent avis.

10. En suivant cette approche, le CEPD entend veiller à ce que le développement des systèmes RFID et leur domestication tiennent compte des préoccupations légitimes en matière de protection des données et de la vie privée.

III. RECENSEMENT DES CONSÉQUENCES

Systèmes et étiquettes RFID

11. Bien que — comme nous l'avons dit plus haut — cette technologie soit en pleine évolution et que son aboutissement soit incertain, il est tout à fait possible de décrire les principales caractéristiques de cette évolution en vue d'en déterminer les conséquences en termes de protection des données.

([1]) Document WP 136, publié sur le site du groupe.
([2]) Communication du 7 mars 2007 de la Commission au Parlement européen et au Conseil — Suivi du programme de travail pour une meilleure mise en application de la directive sur la protection des données [COM (2007) 87 final].
([3]) JO C 255 du 27.10.2007, p. 1 intitulé «Avis sur la communication relative à la directive sur la protection des données».
([4]) Proposition du 13 novembre 2007 de directive du Parlement européen et du Conseil modifiant la directive 2002/22/CE concernant le service universel et les droits des utilisateurs au regard des réseaux et services de communications électroniques, la directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques et le règlement (CE) nº 2006/2004 relatif à la coopération en matière de protection des consommateurs [COM(2007) 698 final]. La directive 2002/58/CE est dénommée ci-après «la directive vie privée et communications électroniques».
([5]) http://www.rfidconsultation.eu/

12. Il est à cet égard de la plus haute importance de ne pas se limiter aux seules étiquettes, mais d'envisager l'infrastructure RFID dans sa globalité, à savoir l'étiquette, le lecteur, le réseau, la base de données de référence et la base de données dans laquelle les données produites par l'association étiquette — lecteur sont conservées. Comme cela a été brièvement souligné dans la partie introductive de la communication, les systèmes RFID ne sont pas de simples «étiquettes électroniques»; c'est pourquoi les questions relatives à la protection des données ne se limitent pas exclusivement aux étiquettes, mais s'étendent à tous les éléments de l'infrastructure globale des RFID. En effet, chacun de ceux-ci a un rôle à jouer et contribue, au besoin, à la mise en œuvre du cadre légal européen en matière de protection des données. Ces éléments évolueront en fonction des principales tendances qui se manifesteront au sein de la société de l'information en développement, telles qu'une bande passante presque illimitée, un réseau de communications omniprésent et une capacité de stockage sans limite.

Incidence des systèmes et des étiquettes RFID

13. Bien qu'il soit nécessaire, comme souligné au point précédent, d'adopter une approche plus générale, plusieurs raisons justifient de commencer par se pencher sur l'utilisation de la RFID à des fins d'étiquetage d'articles de consommation, comme dans le secteur de la distribution. Il est évident que l'étiquetage sera de plus en plus utilisé à l'avenir et que cette technologie connaîtra bientôt une application généralisée. Contrairement à d'autres applications RFID, dont l'usage est restreint ou limité, l'étiquetage d'articles de consommation est en passe de devenir une application de masse; bon nombre de produits de consommation sont d'ores et déjà pourvus d'une étiquette RFID. Cette évolution aura inévitablement des incidences pour un grand nombre de personnes, dont les données à caractère personnel seront vraisemblablement traitées chaque fois qu'ils achèteront un produit sur lequel est apposée une étiquette RFID.

14. Il conviendrait d'accorder une attention particulière aux conséquences de l'étiquetage RFID pour les propriétaires de produits. Les systèmes RFID risquent de donner des «prolongements» à la relation entre un produit et son propriétaire en classant ce dernier parmi les personnes «disposant d'un faible budget» ou «disposant d'un budget attrayant», pour des transactions futures; attribuer un numéro unique de manière excessive ([1]) pourrait mener à une «sanction» automatique de certains comportements (obligation de recyclage, déchets, etc.). Or, les personnes ne devraient pas faire l'objet de décisions automatisées à leur encontre. Cette capacité propre à la technologie RFID accroît le risque que la société de l'information devienne le lieu où des décisions automatisées seront prises et où la technologie sera utilisée à mauvais escient pour réglementer le comportement humain.

15. Les données enregistrées ou générées par une étiquette RFID peuvent être des données à caractère personnel, telles qu'elles sont définies à l'article 2 de la directive sur la protection des données. Par exemple, les cartes à puce utilisées pour voyager peuvent contenir des informations relatives à l'identité de la personne, ainsi que des informations relatives à ses derniers déplacements. Si un individu peu scrupuleux souhaitait localiser des personnes, il lui suffirait de placer, à des endroits stratégiques, des lecteurs qui pourraient lui donner des informations sur les déplacements des titulaires de cartes, ce qui aurait pour effet de violer la vie privée et la confidentialité des informations à caractère personnel des personnes concernées.

16. Ces risques pourraient surgir même si les informations contenues dans l'étiquette RFID ne comportaient pas le nom des personnes. Les étiquettes RFID contiennent des identifiants uniques attribués aux produits de consommation: si chaque étiquette en est pourvue, ce code d'identification peut être utilisé à des fins de surveillance. Par exemple, si une personne porte une montre pourvue d'une étiquette RFID contenant un code d'identification, ce code pourrait également servir d'identifiant unique pour le porteur de la montre, même si son identité est inconnue. L'applicabilité de la directive dépendrait de la manière dont les informations sont utilisées et mises en relation avec la montre elle-même ou avec la personne. La directive s'appliquerait, par exemple, si des informations concernant la localisation des personnes étaient générées et qu'elles étaient susceptibles d'être utilisées pour surveiller le comportement de celles-ci ou, par exemple, pratiquer une différenciation des prix, refuser un accès ou exposer à une publicité non souhaitée.

17. À cet égard, il convient de veiller à ce que le déploiement des applications RFID s'accompagne des mesures techniques nécessaires pour minimiser le risque de divulgation non souhaitée d'informations. Ces mesures peuvent notamment consister à exiger que les infrastructures RFID, en particulier les étiquettes RFID, soient conçues de manière à prévenir ce problème. Par exemple, les étiquettes RFID peuvent être conçues avec une commande d'effaçage («kill command») permettant leur désactivation. Cette option fera l'objet d'un examen plus approfondi au chapitre IV du présent avis.

18. Le fait que les systèmes RFID offrent la possibilité de suivre les produits après leur vente soulève de nouvelles questions dans le débat sur la vie privée. Il conviendra, en effet, de tenir compte de deux éléments dans l'analyse de l'incidence de la technologie RFID, à savoir dans quelle mesure l'article est considéré comme présentant un caractère personnel et la mobilité de cet article ([2]).

19. Le cycle de vie d'un objet pourrait également compléter l'analyse de risque requise et contribuer à l'évaluation quantitative des risques potentiels pour la vie privée. Étant donné qu'il existe un risque qu'une étiquette ne soit pas désactivée, un produit d'utilisation finale ayant un cycle de vie long pourra collecter davantage de données concernant son propriétaire et en établir un profil plus précis. En revanche, un produit ayant un cycle de vie court, entre sa production et son recyclage, comme une cannette de soda, devrait présenter moins de risques et pourrait dès lors nécessiter des mesures moins strictes qu'un produit ayant un cycle de vie beaucoup plus long.

([1]) Dr. Sarah Spiekermann, directrice du Centre de Recherche de Berlin sur l'économie liée à Internet, atelier sur la RFID et l'informatique omniprésente, organisé par le Dialogue transatlantique des consommateurs le 13 mars 2007.

([2]) Dara J. Glasser, Kenneth W. Goodman and Norman G. Einspruch, Chips, tags and scanners: Ethical challenges for radio frequency identification, Ethics and Information Technology, Volume 9, No. 2/2007.

Questions relatives à la vie privée et à la protection des données en ce qui concerne le déploiement du système RFID

20. Afin de mieux appréhender les conséquences des systèmes RFID sur la vie privée et la protection des données, il convient de distinguer cinq questions essentielles relatives à la vie privée et à la sécurité.

21. La première question porte sur l'identification de la personne concernée. Il y a plus de soixante ans, l'étiquette RFID avait pour but d'identifier l'ami ou l'ennemi. De nos jours, les systèmes RFID sont en mesure non seulement de reconnaître les caractéristiques générales d'un objet, mais peuvent aller jusqu'à permettre l'identification d'un individu, ce qui doit par conséquent se faire dans le respect de la vie privée.

22. La deuxième question concerne l'identification des personnes responsables du traitement des données. Cette identification, telle qu'elle est prévue à l'article 2, point d), de la directive sur la protection des données, pourrait être plus difficile dans le cas des systèmes RFID et la question nécessite donc un examen plus approfondi. L'identification du responsable du traitement demeure une étape cruciale pour établir les responsabilités de chacun des acteurs concernés qui sera appelé à se conformer au cadre légal existant en matière de protection des données. Au cours du cycle de vie de l'étiquette, le responsable du traitement pourrait changer plusieurs fois en fonction des services supplémentaires qui pourraient être fournis en rapport avec l'objet étiqueté.

23. La troisième question est liée au fait que la distinction traditionnelle entre sphère privée et sphère publique perd de sa substance. Même si cette distinction n'était pas non plus toujours bien nette dans le passé, la plupart des gens sont conscients des limites qui existent entre les espaces privés et publics (et des zones grises) et prennent des décisions éclairées ou intuitives afin d'adapter leur comportement en conséquence. Selon Hall [1], l'espace personnel se traduit généralement par la distance physique qui s'établit entre des personnes. La gestion de la vie privée peut également être considérée comme un processus dynamique de régulation de ces limites [2]. Il n'est dès lors pas surprenant que l'aspect «communication sans fi»l de l'étiquette, ainsi que la capacité de lecture hors de portée visuelle qui la caractérise, suscitent des inquiétudes en termes de respect de la vie privée, en ce qu'ils rendent floues ces limites traditionnelles et leur gestion. Ce qui est redouté, en fait, c'est que l'individu perde tout ou partie du contrôle de la gestion de la distance qu'il exerçait jusqu'ici. En conséquence, la distance de lecture des premières applications de systèmes RFID a été la cible tant des partisans que des détracteurs de cette technologie.

24. La quatrième question se rapporte à la taille et aux propriétés physiques des étiquettes RFID. Étant donné que l'étiquette doit essentiellement être de petite taille et peu coûteuse, les mesures de sécurité qui pourraient être déployées sur cette partie du système RFID seront par définition limitées. Or, l'aspect «communication sans fil» accroît le niveau de risque par rapport à une communication avec fil, si bien que des mesures de sécurité supplémentaires sont requises.

25. La cinquième question concerne le manque de transparence du traitement. Les systèmes RFID peuvent donner lieu, à l'insu du consommateur, à une collecte et à un traitement d'informations qui pourraient être utilisées pour établir son profil. Cette conséquence peut parfaitement être illustrée en comparant les systèmes RFID au téléphone mobile — une comparaison qui est d'ailleurs fréquente: d'une part, le téléphone mobile a bénéficié d'un degré très élevé d'acceptation technologique, indépendamment des risques potentiels d'intrusion dans la vie privée, et on pourrait en conclure que la RFID sera acceptée de la même manière; d'autre part, il convient de souligner que le téléphone mobile est un objet visible, qui est toujours sous le contrôle de l'utilisateur final étant donné qu'il peut être éteint et que tel n'est pas le cas avec la RFID.

26. Même si la collecte et le traitement d'informations effectués à l'insu du consommateur peuvent être légitimes, il est également possible et, dans certains cas, tout aussi probable, qu'ils soient illégitimes.

27. Les explications fournies dans le présent chapitre conduisent à la conclusion suivante:l'application de la technologie RFID à grande échelle est un phénomène essentiellement nouveau, qui est susceptible d'avoir des répercussions importantes sur notre société et sur la protection des droits fondamentaux au sein de celle-ci, notamment en matière de vie privée et de protection des données. La RFID peut entraîner un changement qualitatif.

IV. QUALIFICATION DES CONSÉQUENCES

Introduction

28. Le présent chapitre sera principalement axé sur l'incidence de la technologie RFID sur la protection des droits fondamentaux dans notre société, notamment sur la protection de la vie privée et des données. Cette question sera abordée en deux étapes: la première consistera à donner une brève description de la manière dont ces droits fondamentaux sont protégés par le cadre juridique actuel; dans la seconde partie, le CEPD réfléchira aux possibilités d'exploiter pleinement le cadre juridique actuel. Cette éventualité a été intégrée dans l'avis relatif à la communication sur la directive sur la protection des données par les termes «mise en œuvre intégrale des dispositions actuelles de la présente directive».

29. Le point de départ est le suivant: les nouvelles évolutions technologiques, notamment les systèmes RFID, ont des répercussions évidentes sur les exigences liées à un cadre juridique efficace régissant la protection des données. La nécessité de prévoir une protection effective des données à caractère personnel d'une personne peut également entraîner l'imposition de limitations par rapport à l'utilisation de ces nouvelles technologies. L'interaction peut donc se résumer comme suit: la technologie influe sur la législation, qui, à son tour, a une incidence sur la technologie [3].

[1] Edward T. Hall, 1966, La dimension cachée (1ère éd.), Garden City, N.Y: Doubleday.

[2] Altman, I., 1975, The Environment and Social Behaviour, Brooks/Cole Monterrey.

[3] Voir les observations du CEPD de mars 2006 relatives à la communication de la Commission sur l'interopérabilité des bases de données européennes, publiées sur le site Internet du CEPD.

Protection des droits fondamentaux

30. La protection des droits fondamentaux à la vie privée et à la protection des données au sein de l'Union européenne est garantie en premier lieu par un cadre législatif, nécessaire du fait qu'il s'agit de droits consacrés par l'article 8 de la Convention européenne des droits de l'homme et des libertés fondamentales, ainsi que par les articles 7 et 8 de la Charte des droits fondamentaux de l'Union. Le cadre législatif pertinent en matière de protection des données et de RFID est essentiellement la directive 95/46/CE relative à la protection des données et la directive 2002/58/CE «vie privée et communications électroniques» ([1]).

31. Le cadre législatif général en matière de protection des données, tel qu'il est défini dans la directive 95/46/CE, s'applique à la technologie RFID pour autant que les données traitées par les systèmes RFID relèvent de la définition des données à caractère personnel. Dans certains cas, les applications RFID traitent manifestement des données à caractère personnel et entrent incontestablement dans le champ d'application de la directive sur la protection des données, mais il existe aussi des applications à l'égard desquelles l'applicabilité de la directive sur la protection des données peut ne pas être aussi évidente. L'avis n° 4/2007 rendu par le Groupe de l'article 29 sur le concept de données à caractère personnel a pour objectif de contribuer à assurer une meilleure interprétation du concept de données personnelles, à faire en sorte que celle-ci soit communément reconnue et, par là même, à réduire le degré d'incertitude qui entoure cette notion ([2]).

32. En ce qui concerne la directive «vie privée et communications électroniques», la situation se présente comme suit. Dans l'état actuel des choses, il est difficile de savoir si cette directive est applicable aux applications RFID. C'est pour cette raison que la proposition de la Commission du 13 novembre 2007 visant à adapter la directive comporte une disposition destinée à préciser que la directive s'applique effectivement à certaines applications RFID. Cependant, d'autres applications RFID risquent de ne pas entrer dans son champ d'application parce que la directive est limitée au traitement de données à caractère personnel dans le cadre de la fourniture de services de communications électroniques accessibles au public dans des réseaux publics de communications.

33. La protection des données à caractère personnel peut être complétée par un éventail d'instruments d'autoréglementation (cadre non législatif). Le recours à ce type d'instruments est activement favorisé dans les deux directives, en particulier à l'article 27 de la directive sur la protection des données, qui précise que les États membres et la Commission encouragent l'élaboration de codes de conduite destinés à contribuer à la bonne application de la directive. En outre, les instruments d'autoréglementation pourraient contribuer efficacement à la mise en œuvre des mesures de sécurité requises par l'article 17 de la directive sur la protection des données et par l'article 14 de la directive «vie privée et communications électroniques».

Mise en œuvre intégrale du cadre existant

34. L'avis sur la communication relative à la directive sur la protection des données énumère une série d'instruments qui sont disponibles et pourraient permettre de contribuer à une meilleure mise en œuvre de la directive. La plupart des instruments non contraignants mentionnés dans cet avis sont applicables à la technologie RFID, notamment les communications interprétatives ou les autres communications, la promotion des meilleures pratiques, l'utilisation des labels de protection de la vie privée et la réalisation d'audits par des tiers. La possibilité d'adopter des règles spécifiques en matière de RFID sera examinée au chapitre V, mais des améliorations peuvent également être apportées à l'intérieur du cadre juridique existant.

Instruments d'autoréglementation

35. Le CEPD convient avec la Commission qu'il convient, dans un premier temps, d'autoriser l'autoréglementation en permettant aux parties concernées de créer à bref délai un environnement conforme au cadre juridique, ce qui contribuera à créer un environnement juridique plus sûr.

36. La Commission devrait, en concertation avec le Groupe des parties prenantes sur les RFID, stimuler et piloter ce processus d'autoréglementation. À cet égard, le CPDE attend avec intérêt la recommandation annoncée dans la communication, qui devrait contenir des orientations spécifiques établissant «les principes que les pouvoirs publics et autres parties concernées devront appliquer en matière d'utilisation de la RFID».

37. Selon la communication, l'autoréglementation pourrait prendre la forme d'un code de conduite ou d'un code de bonnes pratiques. Le CEPD estime que, quelle qu'en soit la forme, l'autoréglementation devrait:

— fournir des orientations concrètes et pratiques sur des types particuliers d'applications RFID et ainsi contribuer à faire respecter le cadre juridique existant en matière de protection des données,

— traiter des questions et problèmes propres à la protection des données qui se posent dans le cadre des applications RFID génériques,

— contribuer à assurer l'application uniforme et harmonisée de la directive sur la protection des données dans l'ensemble de l'UE, en particulier dans un secteur qui est susceptible d'utiliser le même type d'applications RFID dans toute l'Union européenne,

— être appliquée par toutes les parties prenantes. Le non-respect devrait entraîner des conséquences négatives (éventuellement financières).

([1]) Le point 59 du présent avis examinera la pertinence d'une troisième directive, à sa voir la directive 1999/5/CE du Parlement européen et du Conseil du 9 mars 1999 concernant les équipements hertziens et les équipements terminaux de télécommunications et la reconnaissance mutuelle de leur conformité (JO L 91 du 7.4.1999, p. 10).

([2]) Voir notamment p. 10 de l'avis, cite à la note de bas de page 5.

38. Le CEPD attire l'attention sur un cas dans lequel l'autoréglementation sera particulièrement utile. Pour les applications RFID qui impliquent le traitement de données à caractère personnel, la directive sur la protection des données impose diverses obligations au responsable du traitement, en particulier à l'article 17 (sécurité des traitements) et à l'article 7 (obligation de n'effectuer le traitement des données que sur la base de motifs juridiques appropriés). Conformément à ces dispositions, le responsable du traitement doit, d'une part, prendre des mesures contre la diffusion non autorisée des données et, d'autre part, s'assurer que le traitement (le cas échéant, la diffusion des informations via les lecteurs), ne soit effectué qu'avec le consentement informé de la personne concernée.

39. Ces dispositions de la directive sur la protection des données peuvent être interprétées comme reflétant l'exigence que les applications RFID soient déployées en prévoyant les solutions techniques nécessaires pour prévenir ou minimiser les risques de divulgation non souhaitée d'informations et faire en sorte que le traitement ou le transfert de données ne s'effectue qu'avec le consentement informé de la personne concernée, le cas échéant. Le CEPD estime que l'existence de cette obligation (qui impose d'appliquer les solutions techniques nécessaires pour prévenir ou minimiser les risques de divulgation non souhaitée d'informations), avec le caractère contraignant qu'elle revêt dans le cadre du déploiement des applications RFID, sera d'autant plus forte et plus claire si elle est intégrée dans le prochain code de conduite ou dans le code des bonnes pratiques mentionnés plus haut. Pour ces raisons, il recommande vivement d'inclure cette interprétation de la directive sur la protection des données dans la recommandation de la Commission, en mettant l'accent sur l'existence de l'obligation de déployer les applications RFID en prévoyant les mesures techniques nécessaires pour prévenir la collecte ou la divulgation non souhaitées d'informations.

Nécessité d'établir des lignes directrices

40. Le CEPD recommande que la Commission, en concertation étroite avec le groupe des experts RFID, élabore un ou plusieurs documents contenant des lignes directrices claires sur la manière dont il convient d'appliquer le cadre juridique actuel à l'environnement RFID. Ces lignes directrices devraient prévoir les modalités d'application des principes énoncés dans la directive sur la protection des données et la directive vie privée et communications électroniques. Le CEPD formule les suggestions qui suivent en ce qui concerne l'approche globale et le contenu concret de ces lignes directrices.

41. Les lignes directrices fixant les principes applicables à l'utilisation des RFID devraient être suffisamment ciblées et reposer sur une approche sectorielle spécifique. Une approche «passe-partout» ne permettra pas d'atteindre les objectifs recherchés, à savoir la mise en place d'un cadre clair et cohérent. Il convient au contraire de limiter le champ d'application des lignes directrices à des applications sectorielles RFID bien précises.

42. En outre, les lignes directrices devraient proposer des méthodes pratiques et efficaces pour mettre au point des techniques et des normes qui seraient de nature à mettre les systèmes RFID en conformité avec le cadre juridique existant en matière de protection des données et qui impliqueraient l'utilisation de la technologie «privacy by design» (prise en compte du respect de la vie privée dès la conception).

43. Lors de l'application du cadre juridique actuel à l'environnement RFID, il convient d'accorder une attention particulière à l'application des principes relatifs à la protection des données et aux obligations qui incombent au responsable du traitement dans le cas des applications RFID. Les obligations et principes suivants sont particulièrement pertinents:

— le principe du droit à l'information, y compris le droit d'être informé lorsque des données sont collectées par des lecteurs et, dans certains cas, d'être informé de l'étiquetage des produits,

— la notion de consentement, qui est l'un des fondements légaux du traitement de données. Cette notion se concrétise par l'obligation de désactiver les étiquettes RFID au point de vente, à moins que la personne concernée n'ait donné son consentement à une non-désactivation [1]. Le droit de faire désactiver les étiquettes RFID contribue également à assurer la sécurité des informations, c'est-à-dire à garantir que les données traitées par les étiquettes RFID ne seront pas divulguées inopportunément à des tiers,

— le droit des personnes de ne pas faire l'objet de décisions à leur encontre sur la seule base du traitement automatisé d'un profil personnel déterminé.

44. S'agissant du droit à l'information, il conviendrait de préciser dans les orientations que les personnes doivent recevoir des informations sur le traitement de leurs données à caractère personnel. En particulier, elles devraient être averties, notamment, i) de la présence de lecteurs et de la présence d'étiquettes RFID actives sur les produits ou sur leur emballage; ii) des conséquences de la présence de ces étiquettes en termes de collecte d'informations et iii) des finalités pour lesquelles les informations collectées sont destinées à être utilisées.

45. L'utilisation de logos peut être un moyen approprié de fournir l'information. Les logos peuvent être utilisés pour avertir de la présence de lecteurs et d'étiquettes RFID qui sont censées rester actives. Toutefois, l'utilisation des seuls logos ne suffira pas à assurer le traitement loyal des informations, qui exige que les informations soient fournies aux personnes concernées de manière claire et compréhensible. L'utilisation de logos devrait être considérée comme une mesure destinée à compléter la communication d'informations plus détaillées.

[1] Pour plus de détails, voir les paragraphes 46 à 50 du présent avis.

La pierre angulaire: le principe du consentement préalable au traitement des données

46. Pour toutes les applications RFID concernées, les solutions envisagées devraient (et c'est une condition sine qua non) respecter et mettre en œuvre au point de vente le principe du consentement préalable. Il serait illicite de permettre que les étiquettes RFID continuent à transmettre des informations après la vente, sauf si le responsable du traitement peut invoquer des motifs juridiques appropriés à cet effet. Ces motifs devraient en principe être limités aux deux cas suivants: a) si la personne concernée a donné son consentement ou b) si cette divulgation d'informations est nécessaire afin de fournir un service, à la demande spécifique et librement formulée par la personne en question ([1]). Ces deux motifs juridiques pourraient dès lors être considérés comme relevant du principe du consentement préalable.

47. En application du principe du consentement préalable, il conviendrait de désactiver les étiquettes au point de vente, à moins que la personne qui a acheté le produit sur lequel l'étiquette est apposée n'ait exprimé le souhait que le code reste actif. En exerçant le droit de laisser le code actif, la personne donnerait son consentement au traitement ultérieur de ses données, par exemple à la transmission des données au lecteur lors de sa visite suivante chez le responsable du traitement des données.

48. Afin de faire face à la diversité croissante des applications RFID et de faciliter le développement de nouveaux modèles commerciaux innovants, le CEPD souligne qu'il est important d'adopter une approche souple. Il convient donc aussi de faire preuve de souplesse en ce qui concerne la mise en œuvre du principe du consentement préalable.

49. Les possibilités d'application du principe du consentement préalable sont multiples. Par exemple, au lieu de retirer l'étiquette, il pourrait être envisagé de la verrouiller, de la désactiver temporairement ou, conformément à un modèle de sécurité connu sous le nom de «resurrecting duckling model» (modèle de la résurrection du caneton) ([2]), de la rattacher exclusivement à un utilisateur donné. Dans le cas d'une étiquette ayant un cycle de vie court, l'adresse de l'étiquette qui permet de localiser avec précision les informations contenues dans une base de données pourrait également être effacée de la base de données de référence, ce qui permettrait d'éviter le traitement ultérieur des données supplémentaires collectées par l'étiquette.

50. En conclusion, le CEPD fait valoir que, même si le principe du consentement préalable au point de vente constitue une obligation légale qui s'applique déjà dans la plupart des cas en vertu de la directive sur la protection des données, il y a de bonnes raisons de faire figurer cette obligation dans les instruments d'autoréglementation, afin de veiller notamment à ce que ce principe soit appliqué de la manière la plus appropriée. Il convient en tout état de cause de prévoir sa mise en œuvre de manière spécifique pour les applications RFID qui ne rentrent pas dans le champ d'application de la directive sur la protection des données.

Nécessité d'une prise en compte du respect de la vie privée dès la conception

51. Pour réduire à leur minimum les risques pour la vie privée et la protection des données, la communication de la Commission souscrit, au point 3.2 de la page 6, à l'idée de définir et d'adopter des critères dès la conception. Le CEPD accueille favorablement cette approche. En effet, l'adoption de spécifications et de critères de conception, mieux connus sous le nom de meilleures techniques disponibles («MTD»), contribuera efficacement à la réglementation de la protection des données et au respect des exigences en matière de sécurité. La détermination de ces critères technologiques et d'ordre organisationnel, si elle est fréquemment réexaminée, renforcera le modèle que l'Union européenne met au point actuellement en vue de garantir la symbiose entre les exigences en matière de vie privée et celles en matière de sécurité.

52. Il est en outre capital de bien définir les MTD en matière de vie privée et de sécurité qui sont applicables aux systèmes RFID si l'on veut instaurer un environnement fiable propre à renforcer l'adhésion des utilisateurs finaux et à assurer la compétitivité de l'industrie européenne.

53. La sélection des MTD applicables aux systèmes RFID devrait être guidée par des évaluations d'impact en termes de vie privée et de sécurité, travail auquel des efforts doivent encore être consacrés. Le CEPD estime que l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA), ainsi que les centres communs de recherche de la Commission européenne, en association avec les acteurs concernés de l'industrie, peuvent contribuer au recensement des meilleures pratiques et à l'élaboration de méthodologies en la matière. En lançant récemment le projet «orientations directrices techniques RFID», l'office fédéral allemand pour la sécurité en matière de technologies de l'information (le «BSI») a donné un exemple représentatif de MTD ([3])qui pourraient à présent être élaborées au niveau européen.

54. Les normes peuvent également jouer un rôle déterminant dans l'adoption rapide du principe de la prise en compte du respect de la vie privée dès la conception. La Commission devrait dès lors apporter son soutien à l'adoption de garanties en matière de vie privée et de protection des données lors de l'élaboration de normes internationales applicables aux RFID. Dans son document de travail ([4]) sur les RFID, le Groupe de l'article 29 a clairement mis en évidence le fait que les normes puissent contribuer à la prise en compte du respect de la vie privée lors de l'élaboration de systèmes RFID.

([1]) Dans certaines applications RFID, il peut être possible de se baser sur d'autres motifs, tels que l'article 7, point f), (intérêts légitimes du responsable du traitement, sous réserve de garanties appropriées).

([2]) Le nom de ce modèle mis point par Frank Stajano et Ross Anderson de l'Université de Cambridge a été inspiré par le principe selon lequel «le caneton qui brise sa coquille suppose que la première chose qu'il voit bouger doit être sa mère».

([3]) http://www.bsi.bund.de/veranst/rfid/index.htm

([4]) Document de travail (WP 105) relatif aux questions de protection des données liées à la technologie RFID, adopté le 19 janvier 2005.

55. En outre, le CEPD se déclare satisfait de la position adoptée par la Commission en ce qui concerne la recherche et le développement dans le domaine des technologies RFID et la nécessité de réduire les risques pour la vie privée. Le principe de la prise en compte du respect de la vie privée dès la conception doit effectivement être introduit au stade le plus précoce du développement des technologies si l'on veut s'assurer que celles-ci respectent le cadre juridique existant en matière de protection des données. Comme il l'a brièvement indiqué dans son rapport annuel 2006, le CEPD s'associera à cet effort en fournissant, au cas par cas, des avis et des recommandations concernant les projets élaborés dans le cadre du septième programme-cadre (2007-2013).

V. L'ADOPTION DE MESURES LÉGISLATIVES SPÉCIFIQUES EST-ELLE NÉCESSAIRE?

56. L'autoréglementation risque de ne pas suffire pour assurer la mise en œuvre intégrale du cadre existant en matière de protection des données et de la vie privée. Même si elle répond aux exigences mentionnées plus haut, sa mise en application s'effectue sur une base volontaire et le non-respect de ses dispositions risque de ne pas toujours être sanctionné efficacement. En outre, des mesures législatives contraignantes pourraient s'avérer nécessaires afin d'assurer le respect des droits des personnes à la protection de la vie privée et des données — et ce d'autant plus en cas d'échec de l'approche fondée sur l'autoréglementation.

57. Un point essentiel consiste à déterminer quels sont les instruments juridiques permettant de veiller à ce que les applications RFID soient effectivement déployées avec les solutions techniques nécessaires pour prévenir ou minimiser les risques en matière de protection des données et de la vie privée et à ce que les responsables du traitement compétents prennent les mesures adéquates afin de remplir les obligations qui leur incombent en vertu des cadres juridiques existants. Ce point suscite d'autres interrogations:

— Est-il nécessaire d'adopter des règles spécifiques?

— Dans l'affirmative, ces règles peuvent-elles être adoptées au sein du cadre législatif existant, par exemple en recourant aux procédures de comitologie en vigueur?

— Ou convient-il plutôt d'élaborer un nouvel instrument législatif en vue d'assurer le déploiement effectif d'une application RFID pourvue de technologies intégrées renforçant la protection de la vie privée?

58. Le présent chapitre est consacré à l'examen des possibilités d'adopter des mesures législatives contraignantes au sein du cadre juridique en place; le chapitre VI traitera — parce qu'il s'agit d'une question à part entière — de la nécessité d'adopter un nouvel instrument législatif pour les RFID.

59. En premier lieu, il convient d'accorder une attention particulière à l'article 17 de la directive 95/46/CE, à l'article 14, paragraphe 3, de la directive 2002/58/CE et à l'article 3, paragraphe 3, point c), de la directive 1999/5/CE. L'article 14, paragraphe 3, autorise les États membres à adopter des mesures 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 ([1]). La directive 1999/5/CE dispose, en son article 3, paragraphe 3, point c), que la Commission peut décider — conformément à la procédure de comitologie — que les appareils relevant de certaines catégories d'équipements ou certains types d'appareils sont construits de sorte qu'ils comportent des sauvegardes afin d'assurer la protection des données à caractère personnel et de la vie privée des utilisateurs et des abonnés. Or, cette disposition n' a pas été utilisée jusqu'ici.

60. Les dispositions décrites ci-dessus habilitent le législateur — tant national que communautaire — à exiger que les garanties en matière de vie privée et de protection des données soient prises en compte dès la fabrication de systèmes RFID: c'est le principe de la prise en compte du respect de la vie privée dès la conception, ([2]) qui préconise également le recours aux meilleures techniques disponibles.

61. Afin de rendre ce principe obligatoire, le CEPD recommande que la Commission ait recours au mécanisme prévu à l'article 3, paragraphe 3, point c), de la directive 1999/5/CE, en consultation avec le groupe d'experts sur les RFID.

62. En deuxième lieu, il est possible de préciser, en apportant des modifications aux directives elles-mêmes, que le cadre législatif actuel s'applique aux RFID. Comme nous l'avons dit, la Commission vient de présenter une proposition visant à modifier la directive «vie privée et communications électroniques», en y incluant une nouvelle disposition à cet effet. Le CEPD se félicite de cette première confirmation de l'applicabilité de la directive aux applications RFID. Il traitera des problèmes spécifiques que soulève la relation entre la directive «vie privée et communications électroniques» et les technologies RFID dans son avis sur la proposition de modification, qui sera publié au début de 2008.

63. Compte tenu du fait que la Commission ne prévoit pas de modifier la directive sur la protection des données dans un futur proche ([3]), les possibilités de préciser que le cadre juridique actuel s'applique aux technologies RFID sont limitées.

VI. UN CADRE JURIDIQUE PROPRE AUX RFID EST-IL NÉCESSAIRE?

Intentions de la Commission

64. Dans sa communication ([4]), la Commission met l'accent sur l'importance de la sécurité et de la notion de la prise en compte du respect de la vie privée dès la conception. Elle demande également la participation de toutes les parties

([1]) Et conformément 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 (JO L 36 du 7.2.87, p. 31).
([2]) Voir chapitre IV.
([3]) Le CEPD souscrit à cette approche, voir point 64.
([4]) Au point 4.1.

concernées. Les travaux de la Commission déboucheront essentiellement sur «une recommandation énonçant les principes que les pouvoirs publics et autres parties concernées devront appliquer en matière d'utilisation de la RFID». Celle-ci sera probablement adoptée au printemps de 2008. Les ambitions législatives mentionnées dans la communication comportent deux étapes. La Commission:

— étudiera la possibilité d'ajouter des dispositions appropriées concernant la RFID à la prochaine proposition de modification de la directive «vie privée et communications électroniques». Comme nous l'avons dit précédemment, la Commission a proposé, en novembre 2007, de modifier cette directive afin de confirmer son applicabilité aux RFID ([1]), mais sans proposer d'étendre son champ d'application aux réseaux privés,

— examinera la nécessité de prendre de nouvelles mesures législatives afin de garantir la protection des données et le respect de la vie privée.

65. Cette ligne d'action laisse entendre que la Commission n'envisage pas — du moins pas à court terme — de proposer une nouvelle législation spécifique visant à garantir la protection des données et le respect de la vie privée dans le domaine des RFID.

Paramètres pour le législateur

66. Dans son avis sur la communication relative à la directive sur la protection des données, le CEPD a énuméré quelques grandes orientations concernant les activités législatives à mener dans le domaine du traitement des données à caractère personnel, qui peuvent se résumer comme suit:

— en premier lieu, il conviendrait de maintenir en vigueur les principes essentiels régissant la protection des données: «Il n'est pas nécessaire d'élaborer de nouveaux principes; en revanche, il faut de toute évidence prévoir d'autres arrangements administratifs qui, d'une part, soient efficaces et adaptés à une société fonctionnant en réseau et, d'autre part, permettent de réduire au maximum les coûts administratifs» ([2]),

— en deuxième lieu, des propositions législatives ne devraient être présentées que si leur caractère nécessaire et proportionné est suffisamment démontré. C'est pourquoi le cadre législatif général en vigueur en matière de protection des données ne devrait pas être modifié à court terme,

— en troisième lieu, les évolutions observées dans la société pourraient nécessiter des cadres juridiques spécifiques afin d'adapter les principes de la directive sur la protection des données aux problèmes soulevés par des technologies spécifiques, telles que les RFID. Il est évident que, dans ce contexte également, les conditions de nécessité et de proportionnalité doivent être remplies.

67. Il est utile de préciser, à titre d'étape suivante, les attentes auxquelles le législateur est confronté dans le domaine des RFID, à savoir:

— il faut que la législation soit souple et laisse une marge de manœuvre pour les innovations et le développement technologique. Elle devrait donc être suffisamment neutre sur le plan technique,

— en deuxième lieu, la législation doit assurer la sécurité juridique. Elle devrait donc être suffisamment spécifique. Il faut que les parties concernées connaissent précisément les règles qui régissent leur comportement,

— en troisième lieu, la législation doit effectivement protéger tous les intérêts légitimes qui sont en jeu. Cela exige en tout état de cause sa mise en application et une définition claire des responsabilités: quelle partie doit répondre de quel comportement ([3])? Ces exigences sont d'autant plus importantes que le respect de la vie privée et la protection des données sont en jeu et qu'il s'agit de droits fondamentaux consacrés par la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales et par la Charte des droits fondamentaux de l'Union européenne.

Point du vue du CEPD

68. Pour le CEPD, il est évident que le législateur européen ne doit pas réagir à chaque développement technologique. En effet, les évolutions technologiques peuvent être rapides, alors que l'adoption et l'entrée en vigueur d'une législation prend (et doit prendre) du temps, car un acte législatif doit être le fruit d'un compromis entre tous les intérêts en jeu. Lorsque l'instrument choisi est une directive, il faut encore plus de temps, puisque celle-ci doit être pleinement mise en œuvre dans les systèmes juridiques des États membres.

69. Toutefois, les RFID ne constituent pas, comme cela a été souligné à plusieurs reprises dans le présent avis, une simple évolution technologique parmi d'autres. La communication décrit les RFID comme la porte d'entrée vers une nouvelle phase de développement de la société de l'information, souvent appelée «internet des objets», et les étiquettes RFID constitueront les éléments essentiels des environnements «intelligents» qui constituent également des étapes importantes dans le développement de ce que l'on appelle souvent la «société de la surveillance» ([4]). Dans ce contexte, une action législative dans le domaine des RFID peut se justifier. Les RFID peuvent entraîner un changement qualitatif.

([1]) Voir à cet égard le nouvel article 3 proposé pour la directive 2002/58/CE.

([2]) Point 24 de l'avis sur la communication relative à la directive sur la protection des données.

([3]) Transposée dans la terminologie utilisée en matière de protection des données, cette question implique l'identification du «responsable du traitement».

([4]) Ce message a été réitéré dans une déclaration des responsables de la protection des données, adoptée à Londres le 2 novembre 2006, disponible sur le site Internet du CEPD: http://www.edps.europa.eu/EDPSWEB/edps/lang/fr/pid/51

70. Dans cette perspective, le CEPD recommande d'envisager l'adoption d'une (proposition de) législation communautaire qui régirait les principales questions relatives à l'utilisation des RFID dans les secteurs concernés, pour le cas où l'on ne parviendrait pas à assurer la bonne application du cadre juridique existant. Après son entrée en vigueur, cette mesure législative devrait être considérée comme une lex specialis par rapport au cadre général existant en matière de protection des données.

71. L'adoption de cet instrument législatif offrirait les avantages suivants:

— l'instrument pourrait fixer les paramètres essentiels applicables aux mécanismes d'autoréglementation,

— la perspective de son adoption pourrait s'avérer une manière efficace d'inciter les parties prenantes à mettre en place des mécanismes d'autoréglementation offrant une protection appropriée.

72. Plus concrètement, la Commission pourrait être invitée à élaborer un document de consultation décrivant les avantages et les inconvénients d'une législation spécifique, ainsi que ses principaux éléments. Les parties concernées pourraient bien entendu être invitées à apporter leur contribution à cette consultation. De même, le Groupe de l'article 29 pourrait être associé aux travaux.

Modalités éventuelles

73. L'intervention du législateur pourrait offrir un cadre juridique «sur mesure», comprenant divers instruments réglementaires qui viendraient préciser et compléter le cadre juridique actuel. Ce cadre devrait reposer sur les principes reconnus en matière de protection des données et accorder une place importante à la répartition des responsabilités et à l'efficacité des mécanismes de contrôle.

74. Une raison précise qui pourrait justifier la création d'un cadre législatif spécifique est le fait que toutes les applications RFID n'impliquent pas le traitement de données à caractère personnel. En d'autres termes, lorsque les applications RFID n'impliquent pas le traitement de données à caractère personnel, les parties concernées par la fabrication et la vente de produits utilisant les technologies RFID ne sont pas tenues en droit de mettre en œuvre des mesures technologiques afin d'empêcher l'écoute ou l'installation de lecteurs sans que les personnes en aient été dûment avisées. Pourtant, comme nous l'avons montré, ce type d'application RFID présente également des risques pour la vie privée découlant de la surveillance éventuelle des personnes; il convient donc de prévoir ici le même type de garanties en matière de respect de la vie privée. Concrètement, tel peut être le cas lors de l'étiquetage d'un article de consommation avant son arrivée au point de vente. En résumé, les applications RFID qui n'impliquent pas le traitement de données à caractère personnel sont néanmoins toujours susceptibles de constituer un risque pour le respect de la vie privée des personnes, puisqu'elles laissent une porte ouverte à la surveillance clandestine et à l'utilisation des informations à des fins inacceptables.

75. Le CEPD estime qu'il conviendrait d'éviter cette situation regrettable. Étant donné que la législation actuelle est en partie insuffisante — du moins en ce qui concerne les applications RFID n'impliquant pas de traitement de données à caractère personnel — pour faire face aux risques pour la vie privée et compte tenu du fait que la législation non contraignante présente des lacunes, il s'avère nécessaire de recourir à des mesures législatives impératives pour obtenir un résultat satisfaisant.

76. Ces mesures devraient en tout cas:

— établir que le principe du consentement préalable donné au point de vente constitue une obligation légale concrète et incontournable, y compris pour les applications RFID qui ne rentrent pas dans le champ d'application de la directive sur la protection des données ([1]),

— disposer que le déploiement des applications RFID doit obligatoirement s'effectuer avec les caractéristiques techniques appropriées, autrement dit conformément au principe de la prise en compte du respect de la vie privée dès la conception.

VII. **LA QUESTION DE LA GESTION DES RFID**

77. La communication n'aborde la dimension «transfrontière par essence» des systèmes RFID que dans le cadre du marché intérieur, mais le CEPD estime que la question doit être envisagée dans une optique plus internationale. Dans un magasin, les systèmes RFID sont d'ores et déjà une technologie transfrontière, puisque l'activité de l'étiquette risque de ne pas s'arrêter au point de vente. Au niveau du système RFID global, ces technologies deviennent également transfrontières lorsqu'elles sont susceptibles de donner lieu à un transfert de données à caractère personnel vers un pays tiers. Tel est le cas si le producteur de l'article étiqueté dans le cadre du système RFID est établi en dehors de l'Union européenne ([2]).

78. D'un point de vue plus prospectif, la gestion des bases de données de référence RFID relatives à l'identité revêt également une importance cruciale pour assurer la bonne application du cadre juridique européen existant en matière de protection des données. Le CEPD, qui estime qu'une nouvelle érosion de ce cadre ne serait pas acceptable, insiste pour qu'une solution soit trouvée.

79. Le CEPD considère la question de la gestion des RFID comme un défi majeur, qui exigera des investissements considérables. Il conviendra de trouver la bonne enceinte de négociation, ainsi que l'infrastructure de gestion la plus appropriée, afin de faire en sorte que les droits en matière de protection des données soient respectés comme il convient dans ces environnements internationaux.

([1]) Il a été avancé au chapitre IV que le principe du consentement préalable donné au point de vente constitue une obligation légale qui existe déjà en application de la directive sur la protection des données.

([2]) Les obligations existant dans le cadre du transfert de données à caractère personnel sont traitées aux articles 25 et 26 de la directive sur la protection des données.

80. Dans cette perspective, le CEPD invite la Commission à communiquer son point de vue sur la question de la gestion des RFID, éventuellement en consultation avec le groupe des parties prenantes RFID.

VIII. **CONCLUSION**

81. Le CEPD accueille favorablement la communication de la Commission sur la RFID, car elle aborde les principales questions qui se posent dans le cadre du déploiement des technologies RFID sans négliger celles — essentielles — qui ont trait à la protection de la vie privée et des données. Il convient que les systèmes RFID pourraient jouer un rôle crucial dans le développement de la société de l'information, phénomène généralement désigné sous le nom d'«internet des objets».

Recensement des conséquences

82. L'application de la technologie RFID à grande échelle est un phénomène essentiellement nouveau, qui est susceptible d'avoir des répercussions importantes sur notre société et sur la protection des droits fondamentaux au sein de celle-ci, notamment en matière de vie privée et de protection des données. La RFID peut entraîner un changement qualitatif.

83. Il convient de distinguer cinq questions essentielles relatives à la vie privée et à la sécurité:

— l'identification de la personne concernée,

— l'identification du responsable du traitement,

— le fait que la distinction traditionnelle entre sphère privée et sphère publique perd de sa substance,

— les conséquences liées à la taille et aux propriétés physiques des étiquettes RFID,

— le manque de transparence du traitement.

Qualification des conséquences

84. Le cadre législatif général en matière de protection des données, tel qu'il est défini dans la directive 95/46/CE, s'applique à la technologie RFID pour autant que les données traitées par les systèmes RFID relèvent de la définition des données à caractère personnel.

85. En ce qui concerne la directive «vie privée et communications électroniques», la proposition de la Commission du 13 novembre 2007 visant à adapter la directive comporte une disposition destinée à préciser que la directive s'applique effectivement à certaines applications RFID. Cependant, d'autres applications RFID risquent de ne pas entrer dans son champ d'application parce que la directive est limitée au traitement de données à caractère personnel dans le cadre de la fourniture de services de communications électroniques accessibles au public dans des réseaux publics de communications.

86. La protection des données à caractère personnel peut être complétée par un éventail d'instruments d'autoréglementation. Il convient d'autoriser l'autoréglementation pour autant:

— qu'elle fournisse des orientations concrètes et pratiques sur des types particuliers d'applications RFID,

— qu'elle traite des questions et problèmes propres à la protection des données qui se posent dans le cadre des applications RFID génériques,

— qu'elle contribue à assurer l'application uniforme et harmonisée de la directive sur la protection des données sur l'ensemble de l'UE,

— qu'elle soit appliquée par toutes les parties prenantes.

87. Le CEPD recommande que la Commission, en concertation étroite avec le groupe des experts RFID, élabore un ou plusieurs documents contenant des lignes directrices claires sur la manière dont il convient d'appliquer le cadre juridique actuel à l'environnement RFID.

88. Les lignes directrices fixant les principes applicables à l'utilisation des RFID devraient être suffisamment ciblées et reposer sur une approche sectorielle spécifique. Elles devraient proposer des méthodes pratiques et efficaces pour mettre au point des techniques et des normes qui seraient de nature à mettre les systèmes RFID en conformité avec le cadre juridique existant en matière de protection des données et qui impliqueraient l'utilisation de la technologie «privacy by design» (prise en compte du respect de la vie privée dès la conception).

89. Le CEPD accueille favorablement l'approche adoptée par la Commission dans sa communication, à savoir souscrire à l'idée de définir et d'adopter des critères dès la conception.

90. Le CEPD estime que, même si le principe du consentement préalable au point de vente constitue une obligation légale qui s'applique déjà dans la plupart des cas en vertu de la directive sur la protection des données, il conviendrait de faire figurer cette obligation dans les instruments d'autoréglementation.

L'adoption de mesures spécifiques est-elle nécessaire?

91. Afin de rendre obligatoire le principe de la prise en compte du respect de la vie privée dès la conception, le CEPD recommande que la Commission ait recours au mécanisme prévu à l'article 3, paragraphe 3, point c), de la directive 1999/5/CE, en consultation avec le groupe d'experts sur les RFID.

92. Le CEPD recommande d'envisager l'adoption d'une (proposition de) législation communautaire qui régirait les principales questions relatives à l'utilisation des RFID dans les secteurs concernés, pour le cas où l'on ne parviendrait pas à assurer la bonne application du cadre juridique existant. Après son entrée en vigueur, cette mesure législative devrait être considérée comme une lex specialis par rapport au cadre général existant en matière de protection des données. Elle devrait également apporter une réponse aux préoccupations en matière de respect de la vie privée et de protection des données qui se posent à propos de certaines applications RFID, telle que l'étiquetage du produit avant son arrivée au point de vente, applications qui n'impliquent pas nécessairement le traitement de données à caractère personnel.

93. La Commission devrait élaborer un document de consultation décrivant les avantages et les inconvénients d'une législation spécifique, ainsi que ses principaux éléments.

94. L'intervention du législateur pourrait offrir un cadre juridique «sur mesure», comprenant divers instruments réglementaires qui viendraient préciser et compléter le cadre juridique actuel. Ces mesures devraient en tout cas:

— établir que le principe du consentement préalable donné au point de vente constitue une obligation légale concrète et incontournable, y compris pour les applications RFID qui ne rentrent pas dans le champ d'application de la directive sur la protection des données ([1]),

— disposer que le déploiement des applications RFID doit obligatoirement s'effectuer avec les caractéristiques techniques appropriées, autrement dit conformément au principe de la prise en compte du respect de la vie privée dès la conception.

La question de la gestion des RFID

95. Le CEPD invite la Commission à communiquer son point de vue sur la question de la gestion des RFID, éventuellement en consultation avec le groupe des parties prenantes RFID.

Fait à Bruxelles, le 20 décembre 2007.

Peter HUSTINX

Contrôleur européen de la protection des données

([1]) Il a été avancé au chapitre IV que le principe de «l'opt-in» au point de vente constituait une obligation légale qui existait déjà en vertu de la directive sur la protection des données.