RECOMMANDATIONS

COMMISSION

RECOMMANDATION DE LA COMMISSION

du 12 mai 2009

sur la mise en œuvre des principes de respect de la vie privée et de protection des données dans les applications reposant sur l'identification par radiofréquence

[notifiée sous le numéro C(2009) 3200]

(2009/387/CE)

LA COMMISSION DES COMMUNAUTÉS EUROPÉENNES,

vu le traité instituant la Communauté européenne, et notamment son article 211,

après consultation du Contrôleur européen de la protection des données,

considérant ce qui suit:

(1) L'identification par radiofréquence (RFID) marque une nouvelle évolution de la société de l'information dans la mesure où les objets équipés de dispositifs micro-électroniques permettant de traiter automatiquement des données appartiennent de plus en plus à la vie quotidienne.

(2) Peu à peu, la RFID se banalise et commence ainsi à faire partie de la vie des gens dans une série de domaines comme la logistique ([1]), les soins de santé, les transports publics, le commerce de détail — en particulier pour une sécurité accrue et un rappel plus rapide des produits —, les loisirs, le travail, les péages routiers, la gestion des bagages et les documents de voyage.

(3) La technologie RFID est à même de devenir un nouveau facteur de croissance et d'emploi et donc de contribuer grandement à la stratégie de Lisbonne. En effet, elle est très prometteuse au niveau économique et peut offrir de nouveaux débouchés commerciaux, engendrer des coûts moindres et des gains d'efficacité, notamment en matière de lutte contre la contrefaçon, de gestion des déchets électroniques et des matériaux dangereux et de recyclage des produits en fin de vie.

(4) La technologie RFID permet de traiter des données, y compris des données à caractère personnel, sur de courtes distances sans contact physique ni interaction visible entre le lecteur ou scripteur et l'étiquette de sorte que cette interaction peut se produire sans que la personne concernée s'en rende compte.

(5) Les applications RFID offrent la possibilité de traiter des données concernant une personne physique identifiée ou identifiable directement ou indirectement. Elles permettent de traiter des données à caractère personnel stockées sur l'étiquette, comme le nom de la personne, sa date de naissance ou son adresse, des données biométriques ou des données mettant en relation un numéro RFID spécifique avec des données à caractère personnel stockées ailleurs dans le système. En outre, il est possible d'utiliser cette technologie pour suivre les personnes en possession d'un ou de plusieurs objets portant un numéro RFID.

(6) Étant donné que la RFID peut être utilisée partout et qu'elle est pratiquement invisible, son déploiement exige d'accorder une attention particulière aux questions relatives à la protection des données et de la vie privée. Aussi faut-il intégrer des fonctions de sécurité de l'information et de respect de la vie privée dans les applications RFID avant leur diffusion généralisée (principe de «sécurité et respect de la vie privée assurés dès la conception»).

(7) La RFID ne pourra procurer les nombreux avantages économiques et sociaux escomptés que s'il est prévu des mesures effectives pour garantir la protection des données à caractère personnel et le respect de la vie privée et des principes éthiques associés qui sont au cœur du débat sur l'adhésion du public à la RFID.

(8) Les États membres et les parties intéressées doivent, surtout maintenant que la RFID est en phase initiale de mise en œuvre, redoubler d'efforts pour que les applications RFID soient contrôlées et que les libertés et droits individuels soient respectés.

([1]) COM(2007) 607 final.

(9) La communication de la Commission du 15 mars 2007 intitulée «L'identification par radiofréquence (RFID) en Europe: vers un cadre politique» [1] annonçait que des précisions et indications seraient fournies, dans une ou plusieurs recommandations de la Commission, sur les questions relatives à la protection des données et de la vie privée soulevées par les applications RFID.

(10) Les droits et obligations concernant la protection des données à caractère personnel et la libre circulation de ces données, prévus par 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 [2] et par 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 (directive vie privée et communications électroniques) [3], s'appliquent intégralement à l'utilisation d'applications RFID traitant des données à caractère personnel.

(11) Les principes posés par 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 [4] doivent s'appliquer au développement des applications RFID.

(12) L'avis du Contrôleur européen de la protection des données [5] donne des indications sur la façon de gérer les produits contenant des étiquettes qui sont fournis aux personnes et préconise de réaliser des évaluations d'impact sur la vie privée et la sécurité pour définir et élaborer les meilleures techniques disponibles afin de garantir le respect de la vie privée et la sécurité des systèmes RFID.

(13) Les exploitants d'application RFID doivent prendre toutes les mesures raisonnables pour faire en sorte que les données ne soient liées à une personne physique, identifiée ou identifiable, par aucun moyen susceptible d'être utilisé par l'exploitant lui-même ou toute autre personne, à moins que ces données ne soient traitées conformément aux principes et règles de droit applicables en matière de protection des données.

(14) La communication de la Commission du 2 mai 2007 intitulée «Promouvoir la protection des données par les technologies renforçant la protection de la vie privée» [6] définit des actions précises pour atteindre l'objectif consistant à limiter le traitement des données à caractère personnel et recourir autant que possible à des données anonymes ou à des pseudonymes en soutenant le développement de ces technologies et leur utilisation par les responsables du traitement des données et les personnes.

(15) La communication de la Commission du 31 mai 2006 intitulée «Une stratégie pour une société de l'information sûre — "Dialogue, partenariat et responsabilisation"» [7] reconnaît que la diversité, l'ouverture, l'interopérabilité, la facilité d'utilisation et la concurrence sont des éléments essentiels d'une société de l'information sûre, souligne le rôle des États membres et des administrations publiques pour ce qui est de sensibiliser davantage et de promouvoir les bonnes pratiques en matière de sécurité et invite les parties intéressées du secteur privé à prendre des initiatives visant à élaborer des systèmes abordables pour la certification de sécurité des produits, processus et services qui répondent à des besoins spécifiques de l'Union européenne, notamment en ce qui concerne le respect de la vie privée.

(16) La résolution du Conseil du 22 mars 2007 relative à une stratégie pour une société de l'information sûre en Europe [8] invite les États membres à accorder l'attention qui convient à la nécessité de prévenir et de combattre les menaces émergentes ou existantes qui pèsent sur la sécurité des réseaux de communications électroniques.

(17) Un cadre de réalisation des évaluations d'impact sur la protection des données et de la vie privée, élaboré au niveau communautaire, garantira que les dispositions de la présente recommandation sont appliquées de façon cohérente dans tous les États membres. Ce cadre doit être élaboré sur la base des pratiques existantes et de l'expérience acquise dans les États membres, dans les pays tiers et lors des travaux menés par l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) [9].

(18) La Commission veillera à définir des orientations au niveau communautaire, sur la base des pratiques existantes et de l'expérience acquise dans les États membres et les pays tiers, sur la gestion de la sécurité de l'information en matière d'applications RFID. Les États membres doivent contribuer à ce processus et encourager les entités privées et les pouvoirs publics à y prendre part.

(19) Une évaluation de l'impact sur la protection des données et de la vie privée, réalisée par l'exploitant préalablement à la mise en œuvre d'une application RFID, fournira les informations requises pour prendre les mesures de sauvegarde appropriées. Ces mesures devront être contrôlées et réexaminées au cours du cycle de vie de l'application RFID.

(20) Dans le secteur du commerce de détail, une évaluation de l'impact sur la protection des données et de la vie privée, réalisée sur les produits contenant des étiquettes qui sont vendus aux consommateurs, doit fournir les informations nécessaires pour déterminer s'il existe un risque probable pour la vie privée ou la protection des données à caractère personnel.

[1] COM(2007) 96 final.
[2] JO L 281 du 23.11.1995, p. 31.
[3] JO L 201 du 31.7.2002, p. 37.
[4] JO L 91 du 7.4.1999, p. 10.
[5] JO C 101 du 23.4.2008, p. 1.
[6] COM(2007) 228 final.
[7] COM(2006) 251 final.
[8] JO C 68 du 24.3.2007, p. 1.
[9] Article 2, paragraphe 1, du règlement (CE) n° 460/2004 du Parlement européen et du Conseil (JO L 77 du 13.3.2004, p. 1).

(21) Le recours à des normes internationales, comme celles élaborées par l'Organisation internationale de normalisation (ISO), à des codes de conduite et à de bonnes pratiques qui soient conformes au cadre réglementaire européen peut faciliter l'adoption de mesures de sécurité de l'information et de respect de la vie privée tout au long du processus d'entreprise basé sur la RFID.

(22) Les applications RFID concernant le grand public, comme les billets électroniques dans les transports publics, exigent des mesures de protection appropriées. Les applications RFID ayant trait aux personnes, car utilisant des données biométriques d'identification ou des données relatives à la santé, par exemple, sont particulièrement sensibles du point de vue de la sécurité de l'information et du respect de la vie privée et exigent donc une attention spéciale.

(23) La société dans son ensemble doit avoir connaissance des droits et obligations applicables relativement à l'utilisation des applications RFID. Les parties concernées par le déploiement de la technologie ont donc la responsabilité de fournir aux personnes des informations concernant l'utilisation de ces applications.

(24) Sensibiliser davantage le public et les petites et moyennes entreprises (PME) aux caractéristiques et possibilités de la RFID permettra à cette technologie de tenir ses promesses économiques tout en limitant le risque qu'elle soit utilisée au détriment de l'intérêt public, donc en renforçant son acceptabilité.

(25) La Commission contribuera à la mise en œuvre de la présente recommandation, directement et indirectement, en facilitant le dialogue et la coopération entre les parties intéressées, notamment au titre du programme-cadre pour l'innovation et la compétitivité établi par la décision n° 1639/2006/CE du Parlement européen et du Conseil [1] et du septième programme-cadre de recherche établi par la décision n° 1982/2006/CE du Parlement européen et du Conseil [2].

(26) La recherche et développement sur les technologies renforçant la protection de la vie privée et les technologies de sécurisation de l'information est essentielle au niveau communautaire pour en promouvoir une plus large adoption dans des conditions acceptables.

(27) La présente recommandation respecte les droits fondamentaux et observe les principes reconnus, en particulier, par la Charte des droits fondamentaux de l'Union européenne. Elle vise notamment à assurer le respect absolu de la vie privée et familiale et la protection des données à caractère personnel,

[1] JO L 310 du 9.11.2006, p. 15.
[2] JO L 412 du 30.12.2006, p. 1.

RECOMMANDE:

Champ d'application

1. La présente recommandation donne aux États membres des indications sur les moyens de concevoir et d'exploiter les applications RFID de façon licite, éthique et socialement et politiquement acceptable, en respectant le droit à la vie privée et en assurant la protection des données à caractère personnel.

2. La présente recommandation donne des indications sur les mesures à prendre concernant le déploiement des applications RFID pour faire en sorte que, lorsque celles-ci sont déployées, la législation nationale transposant les directives 95/46/CE, 1999/5/CE et 2002/58/CE soit respectée le cas échéant.

Définitions

3. Les définitions figurant dans la directive 95/46/CE s'appliquent aux fins de la présente recommandation. Les définitions suivantes s'appliquent également. On entend par:

a) «identification par radiofréquence (RFID)», l'utilisation d'ondes électromagnétiques rayonnantes ou d'un couplage de champ réactif dans une portion de radiofréquences du spectre pour communiquer vers ou à partir d'une étiquette selon différents schémas de modulation et d'encodage afin de lire, de façon univoque, l'identité d'une étiquette de radiofréquence ou d'autres données stockées sur celle-ci;

b) «étiquette RFID» ou «étiquette», soit un dispositif RFID ayant la capacité de produire un signal radio, soit un dispositif RFID qui raccorde, rétrodiffuse ou reflète (selon le type de dispositif) et module un signal porteur reçu d'un lecteur ou scripteur;

c) «lecteur ou scripteur RFID» ou «lecteur», un dispositif fixe ou mobile d'identification et de saisie de données utilisant une onde électromagnétique de radiofréquence ou un couplage de champ réactif pour stimuler et effectuer une réponse de donnée modulée à partir d'une étiquette ou d'un groupe d'étiquettes;

d) «application RFID» ou «application», une application qui traite des données par l'utilisation d'étiquettes et de lecteurs et qui repose sur un système dorsal et une infrastructure de communication en réseau;

e) «exploitant d'application RFID» ou «exploitant», la personne physique ou morale, l'organisme public, l'agence ou tout autre organe qui, seul ou avec d'autres, définit la finalité et les modalités de l'exploitation d'une application, y compris les responsables du traitement des données à caractère personnel utilisant une application RFID;

f) «sécurité de l'information», la préservation de la confidentialité, de l'intégrité et de la disponibilité de l'information;

g) «suivi», toute activité exercée afin de détecter, d'observer, de copier ou d'enregistrer la localisation, les déplacements, les activités ou l'état d'une personne.

Évaluations d'impact sur la protection des données et de la vie privée

4. Les États membres doivent veiller à ce que les entreprises, en collaboration avec les parties intéressées de la société civile, élaborent un cadre d'évaluation de l'impact sur la protection des données et de la vie privée. Ce cadre doit être soumis pour approbation au groupe de travail «article 29» sur la protection des données dans un délai de douze mois à compter de la publication de la présente recommandation au *Journal officiel de l'Union européenne*.

5. Les États membres doivent veiller à ce que les exploitants, nonobstant leurs autres obligations en vertu de la directive 95/46/CE:

a) réalisent une évaluation des incidences de la mise en œuvre de l'application sur la protection des données à caractère personnel et le respect de la vie privée, y compris des possibilités d'utiliser l'application pour suivre une personne. Le niveau de détail de l'évaluation doit être approprié aux risques que l'application peut présenter pour la vie privée;

b) prennent les mesures techniques et organisationnelles appropriées pour assurer la protection des données à caractère personnel et le respect de la vie privée;

c) désignent une personne ou un groupe de personnes chargées de réexaminer les évaluations et l'adéquation constante des mesures techniques et organisationnelles pour assurer la protection des données à caractère personnel et le respect de la vie privée;

d) mettent l'évaluation à la disposition de l'autorité compétente au moins six semaines avant le déploiement de l'application;

e) une fois que le cadre d'évaluation de l'impact sur la protection des données et de la vie privée visé au point 4 est disponible, appliquent les dispositions ci-dessus conformément au cadre.

Sécurité de l'information

6. Les États membres doivent aider la Commission à déterminer quelles applications pourraient présenter un risque pour la sécurité de l'information ayant des conséquences pour le grand public. Concernant ces applications, les États membres doivent veiller à ce que les exploitants, avec les autorités compétentes nationales et les organisations de la société civile, élaborent de nouveaux systèmes ou appliquent des systèmes existants, comme la certification ou l'autoévaluation par l'exploitant, afin de démontrer que le niveau de sécurité de l'information et de protection de la vie privée est approprié aux risques évalués.

Informations et transparence concernant l'utilisation de la RFID

7. Sans préjudice des obligations des responsables du traitement des données et conformément aux directives 95/46/CE et 2002/58/CE, les États membres doivent veiller à ce que les exploitants élaborent et rendent publique, pour chacune de leurs applications, une politique d'information concise, précise et aisément compréhensible. Cette politique d'information doit au moins indiquer:

a) l'identité et l'adresse des exploitants;

b) l'objet de l'application;

c) les données qui doivent être traitées par l'application, en particulier s'il s'agit de données à caractère personnel et si la localisation des étiquettes fera l'objet d'un suivi;

d) un résumé de l'évaluation d'impact sur la protection des données et de la vie privée;

e) les risques probables que l'utilisation d'étiquettes dans l'application peut présenter pour la vie privée, et les mesures que les personnes peuvent prendre pour limiter ces risques.

8. Les États membres doivent veiller à ce que les exploitants prennent des mesures pour informer les personnes de la présence de lecteurs, au moyen d'un signe européen commun élaboré par des organismes européens de normalisation avec l'aide des parties concernées. Le signe doit indiquer l'identité de l'exploitant et un point de contact auquel les personnes peuvent se procurer la politique d'information concernant l'application.

Applications RFID utilisées dans le commerce de détail

9. Au moyen d'un signe européen commun élaboré par des organismes européens de normalisation avec l'aide des parties concernées, les exploitants doivent informer les personnes de la présence d'étiquettes placées sur les produits ou incorporées à ceux-ci.

10. Lors de la réalisation de l'évaluation d'impact sur la protection des données et de la vie privée visée aux points 4 et 5, l'exploitant d'application doit déterminer précisément si les étiquettes placées sur des produits ou incorporées à des produits vendus aux consommateurs par des détaillants qui ne sont pas exploitants de cette application présentent un risque probable pour la vie privée ou la protection des données à caractère personnel.

11. Les détaillants doivent désactiver ou retirer, au point de vente, les étiquettes de leur application à moins que les consommateurs, après avoir pris connaissance de la politique d'information visée au point 7, acceptent que les étiquettes restent opérationnelles. Par désactivation des étiquettes, on entend tout processus qui interrompt les interactions d'une étiquette avec son environnement et qui n'exige pas de participation active du consommateur. La désactivation ou le retrait des étiquettes par le détaillant doivent être effectués sur-le-champ et sans coût pour le consommateur. Les consommateurs doivent pouvoir vérifier que la désactivation ou le retrait sont effectifs.

12. Le point 11 ne s'applique pas s'il ressort de l'évaluation d'impact sur la protection des données et de la vie privée que les étiquettes utilisées dans une application de détail et restant opérationnelles au-delà du point de vente ne présentent pas de risque probable pour la vie privée ou la protection des données à caractère personnel. Néanmoins, les détaillants doivent mettre gratuitement à disposition un moyen aisé de désactiver ou de retirer, immédiatement ou ultérieurement, ces étiquettes.

13. La désactivation ou le retrait des étiquettes ne doit impliquer aucune réduction ni cessation des obligations légales du détaillant ou du fabricant envers le consommateur.

14. Les points 11 et 12 ne s'appliquent qu'aux détaillants qui sont exploitants.

Actions de sensibilisation

15. Les États membres, en collaboration avec les entreprises, la Commission et d'autres parties intéressées, doivent prendre les mesures appropriées pour informer les pouvoirs publics et les entreprises, en particulier les PME, des avantages et des risques potentiels liés à l'utilisation de la technologie RFID et pour les y sensibiliser. Il convient d'accorder une attention particulière aux questions de sécurité de l'information et de respect de la vie privée.

16. Les États membres, en collaboration avec les entreprises, les associations de la société civile, la Commission et d'autres parties intéressées, doivent recenser et fournir des exemples de bonne pratique dans la mise en œuvre d'applications RFID pour informer et sensibiliser le grand public. Préalablement à une plus large adoption de la technologie RFID, les États membres doivent également prendre les mesures appropriées, par exemple lancer des projets pilotes à grande échelle, pour sensibiliser davantage le public à cette technologie et aux avantages, risques et conséquences de son utilisation.

Recherche et développement

17. Les États membres doivent coopérer avec les entreprises, les parties intéressées de la société civile et la Commission pour promouvoir et favoriser l'intégration du principe de «sécurité et respect de la vie privée assurés dès la conception» à un stade précoce de développement des applications RFID.

Suivi

18. Les États membres doivent prendre toutes les mesures nécessaires pour porter la présente recommandation à la connaissance de toutes les parties concernées par la conception et l'exploitation d'applications RFID à l'intérieur de la Communauté.

19. Les États membres doivent informer la Commission, au plus tard vingt-quatre mois après la publication de la présente recommandation au *Journal officiel de l'Union européenne*, des mesures prises pour donner à la suite de la présente recommandation.

20. Dans un délai de trois ans à compter de la publication de la présente recommandation au *Journal officiel de l'Union européenne*, la Commission fournira un rapport sur la mise en œuvre de la recommandation, son efficacité et son impact sur les exploitants et les consommateurs, notamment en ce qui concerne les mesures recommandées aux points 9 à 14.

Destinataires

21. Les États membres sont destinataires de la présente recommandation.

Fait à Bruxelles, le 12 mai 2009.

Par la Commission

Viviane REDING

Membre de la Commission