Avis n° 27/2009 du 28 octobre 2009

Objet: avis d'initiative relatif à la RFID (A/2009/003)

La Commission de la protection de la vie privée ;

Vu la loi du 8 décembre 1992 *relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel* (ci-après LVP), en particulier l'article 29 ;

Vu la Recommandation de la Commission européenne du 12 mai 2009 sur la RFID ;

Vu le rapport de M. Frank ROBBEN ;

Émet, le 28 octobre 2009, l'avis d'initiative suivant :

I. CHAMP D'APPLICATION DE L'AVIS

1. Cet avis émis d'initiative traite de l'utilisation des applications RFID en vue du traitement de données à caractère personnel.

2. La Commission émet cet avis en tenant compte des connaissances actuelles en matière de technologie RFID. Elle se réserve bien sûr le droit de modifier sa position à l'avenir en fonction de l'évolution de cette technologie et de ses expériences dans ce domaine. Le présent avis constitue une analyse globale des applications RFID et n'empêche bien entendu pas que la Commission se prononce sur des dossiers spécifiques.

II. RFID : EXPLICATIONS GENERALES

A. Définition et importance de la RFID

3. La radio frequency identification, l'identification par radiofréquence (abrégée en RFID), est une technologie destinée à stocker et à lire à distance des informations contenues dans ce qu'on appelle des "tags" RFID qui se trouvent sur ou dans des objets ou des êtres vivants. La vision derrière ce progrès technique est de pouvoir identifier distinctement n'importe quel objet dans le monde. L'optimalisation de la "supply chain" par le biais d'une visibilité globale constitue le principal facteur de croissance de cette technologie. Dans ce cadre, le scénario idéal est d'utiliser les bons matériaux dans le bon état, au bon endroit, au bon moment. Un système RFID se compose de trois éléments de base: un "reader" ou lecteur, un RFID tag (ci-après appelé tag) et un système destiné à traiter le flux des données. Le lecteur sert à lire les informations contenues sur la puce du tag. Dans la majorité des cas, cette information est limitée à un numéro d'identification mais peut, en fonction de la capacité de mémoire de la puce, éventuellement aussi contenir des informations supplémentaires. La technologie RFID peut être utilisée de diverses manières en fonction des types de tags et de lecteurs (cf. plus loin).

4. La RFID est déjà utilisée dans de nombreux secteurs à diverses fins. Cette technologie est encore relativement jeune et en plein développement, mais ses possibilités d'application sont diverses et très prometteuses. En voici quelques exemples:

- *Transport* : de nombreuses applications de la technologie RFID ont déjà été mises en place dans les transports publics, par exemple le système MOBIB à Bruxelles. Un autre exemple est celui des clés de voiture qui sont aussi souvent équipées d'un système de ce type (transpondeur).

- *Navigation aérienne*: la technologie RFID peut être utilisée pour le traitement des bagages à l'intérieur d'un aéroport. Les "Boarding passes" peuvent également être équipés d'un tag pour pouvoir déterminer où se trouvent les passagers.

- *Soins de santé* : les systèmes RFID y sont utilisés entre autres pour identifier mes médicaments et lutter contre leur contrefaçon. Pour cela, les produits sont pourvus d'un tag par leur fabricant. Ce tag peut être lu par le pharmacien équipé d'un lecteur. Ces lecteurs constatent que le produit vient bien de son réel fabricant. Une application plus parlante encore à ce niveau concerne ce qu'on appelle la "verichip"[1], une puce RFID implantable chez l'homme, de la taille d'environ 2 grains de riz. Cette puce, approuvée en 2004 par la FDA[2] américaine, peut par exemple contenir les données médicales d'un patient susceptibles d'être utiles en cas d'urgence. Aux Pays-Bas, ce type de puce est déjà utilisé dans un night-club et permet l'identification automatique des visiteurs qui se sont fait implanter la puce. Cette identification automatique permet par exemple d'avoir accès à certains espaces et sert également à la facturation des consommations.

- *Contrôle de sécurité – d'accès* : les billets de banque peuvent également être pourvus de tags destinés à lutter contre leur contrefaçon. La RFID est déjà utilisée dans les passeports, notamment dans le passeport belge. L'accès des personnes à certains espaces peut également être régulé par l'utilisation de la technologie RFID, par exemple en les équipant de ce qu'on appelle une "smart card".

- *Secteur de la distribution / secteur de la production* : ici, cette technologie est utilisée entre autres dans la gestion des stocks, qui permet de suivre les produits dans les systèmes logistiques. Cette façon de procéder accélère le fonctionnement des systèmes logistiques. Elle permet également une facturation plus rapide et protège mieux les produits contre le vol. Elle accélère également l'inventarisation des produits (il suffit de passer avec le lecteur RFID dans les rayons). Et les données, entre autres, du comportement d'achat peuvent être combinées à une carte client et utilisées à des fins marketing. Cette technologie permet aussi de plus facilement contrôler par exemple la fraîcheur et l'origine d'un produit. Enfin, la puce RFID peut également, lorsqu'elle est installée sur un GSM, permettre de payer sans contact dans les magasins, etc. Au Japon, ce système est déjà tellement bien implanté que les gens utilisent leur GSM par exemple pour acheter leurs billets de train. En Belgique, un projet pilote est également en cours dans ce cadre (paiement par GSM sans contact[3]).

---

[1] Voir http://www.verichipcorp.com/ou_businesses.html.

[2] Voir avis du groupe 29 renvoi.

[3] http://www.pingping.be/docs/How_it_works.pdf.

B. Fonctionnement

5. Les tags peuvent être "passifs", "actifs" ou "d'enregistrement de circonstances"[4]. Les tags RFID passifs ne possèdent pas de source d'énergie propre et envoient une réponse en convertissant l'énergie des ondes radio émises par le lecteur. Les tags RFID actifs sont alimentés par une batterie et sont lisibles et inscriptibles avec un lecteur. Les tags actifs envoient généralement leur ID à intervalles réguliers. Les tags d'enregistrement de circonstances possèdent non seulement une batterie, mais également des circuits capables de lire les données diagnostiques et de les envoyer vers un système de capteurs. Les tags surveillent les conditions environnementales, communiquent avec d'autres objets et rassemblent les données qui peuvent être détectées par plusieurs capteurs. Les informations sont ensuite renvoyées au système back-end par le biais d'un logiciel réseau.

6. Les tags RFID se distinguent entre eux par la fréquence qu'ils utilisent. De manière générale, on peut dire : plus la fréquence est élevée, plus la portée de lecture est importante.

7. Il est courant que les tags contiennent un numéro d'identification généralement ineffaçable. Dans un système RFID, il s'agit pratiquement toujours de numéros (chronologiques) uniques. Ces numéros peuvent être déterminés lors de la mise en service des tags en inscrivant le numéro sur le tag à l'aide d'un lecteur ou d'une imprimante. Il est également possible de laisser le choix des tags au producteur.

8. Les avantages de l'application de la RFID sont entre autres :

- un code unique qui permet de suivre en permanence et partout un objet individuel ;
- pas besoin de contact physique (comme dans les cartes bancaires) ;
- pas besoin de ligne lisible (par exemple comme c'est le cas pour les codes-barres)
- des (centaines de) codes peuvent être lus en quelques secondes ;
- les distances de lecture possibles sont nettement supérieures à celles que permettent les codes-barres ;
- la contrefaçon des tags RFID est beaucoup plus complexe que celle des codes-barres.

[4] Voir http://www-05.ibm.com/be/ideasfromibm/rfid/nl/index.html.

9. Désavantages potentiels :

- si le numéro d'identification d'un tag RFID peut être associé à une personne, cet individu peut être localisé et suivi ;
- les possibilités de lecture/écriture d'un tag RFID peuvent permettre de commettre des fraudes qui peuvent passer inaperçues, également à l'égard de personnes ;
- leur grande portée (émission/réception) peut induire la confusion et entraîner la lecture de tags RFID non visés, ce qui peut perturber le traitement des données.

C. IMPACTS POTENTIELS SUR LA VIE PRIVEE[5]

10. Plusieurs applications RFID, telles que décrites plus haut, n'impliqueront jamais le traitement de données à caractère personnel. Dans certaines applications, ce sera néanmoins le cas ou cela pourrait l'être. Nous allons faire ci-après la distinction entre deux situations dans lesquelles il peut être question d'un traitement de données à caractère personnel.

C.1. CROISEMENT DE DONNEES PERSONNELLES AVEC UN TAG

11. Le numéro d'identification du tag peut être lié à des données à caractère personnel / une personne, par exemple le numéro d'identification d'un produit donné peut être lié au client qui a acheté ce produit. Un magasin peut lier les numéros d'identification des produits aux données qui figurent sur les cartes de paiement et à une base de données clients. Ceci pourrait par exemple s'avérer utile dans le cadre du traitement de garantie. Une autre application de la RFID au niveau de la carte client pourrait être de suivre le client dans le magasin et de rassembler des données marketing utiles, notamment le temps passé dans certains rayons, le nombre de visites sans achat, etc.

C.2. PLACEMENT DE DONNEES A CARACTERE PERSONNEL SUR UN TAG

12. Comme déjà expliqué plus haut, la RFID est déjà utilisée dans le secteur des transports. Dans certains aéroports, des projets pilotes sont en cours au niveau du tagage des cartes d'embarquement, ce qui permet de localiser les passagers dans l'aéroport. En Belgique, la carte Mobib est basée sur l'utilisation de la RFID. Les données sont reprises sur la puce de la carte.

---

[5] Voir à ce sujet aussi : Article 29 Groupe de travail protection des données, Document de travail sur les questions de protection des données liées à la technologie RFID (radio-identification), 19 janvier 2005.

III. APPLICABILITE DE LA LOI RELATIVE AU TRAITEMENT DES DONNEES A CARACTERE PERSONNEL (LVP)

A. L'application de la RFID utilise des données à caractère personnel

13. Conformément à l'article 1er, §1er de la LVP, il faut entendre par "données à caractère personnel" toute information concernant une personne physique identifiée ou identifiable, désignée ci-après "personne concernée"; est réputée identifiable une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale.

14. Le tag peut servir au stockage de données à caractère personnel (nom, adresse, …). De plus, le numéro d'identification d'un tag peut également être lié à une personne en particulier. Le tag en soi peut donc dévoiler des informations concernant une personne physique mais les conditions de la collecte peuvent également fournir des informations à caractère personnel supplémentaires (c'est ainsi que le traitement des données concernant l'endroit et le moment de la collecte permet de déterminer la présence d'une personne à un moment donné à un endroit précis).

15. A partir du moment où le lien entre le numéro d'identification du tag et une personne physique peut être établi par le biais de la mise en œuvre de moyens raisonnables par le responsable du traitement ou toute autre personne, il s'agit d'un traitement de données à caractère personnel. Si des données à caractère personnel sont mentionnées sur un tag, il est donc question d'un traitement de données à caractère personnel.

16. Dans les cas précités, la Commission considère l'application RFID en principe comme un traitement de données à caractère personnel.

B. L'application RFID peut constituer un traitement de données sensibles[6]

17. Une application RFID donnée (voir plus haut, par exemple la verichip) peut divulguer des informations sur l'état de santé d'une personne.

[6] Dans le cadre de la protection de la vie privée, les données sensibles sont les données visées aux articles 6, 7 et 8 de la LVP.

18. Lorsque l'application RFID est utilisée pour déduire des informations concernant par exemple l'état de santé d'une personne, ces données doivent être considérées comme des données sensibles.

C. L'utilisation de la RFID implique un traitement de données

19. La LVP définit le "traitement" comme toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction de données à caractère personnel.[7]

20. L'utilisation d'un système RFID suppose la collecte, l'enregistrement et le stockage de données (des données à caractère personnel ou non), et ceci, à l'aide de moyens automatisés.

IV. APPLICATION DES PRINCIPES DE LA LOI RELATIVE AU TRAITEMENT DES DONNEES A CARACTERE PERSONNEL (LVP)

A. Légitimité et proportionnalité[8]

21. Toutes les données à caractère personnel doivent être traitées en vue de finalités déterminées, explicites et légitimes et ne pas être traitées ultérieurement de manière incompatible avec ces finalités.

22. Pour être légitime, toute finalité doit entre autres satisfaire à une des conditions énumérées à l'article 5 de la LVP.

23. Un traitement de données à caractère personnel dans le cadre d'une application RFID est en principe possible lorsque les personnes concernées ont donné leur *consentement*[9]. Ce consentement contribue sans aucun doute à l'acceptation sociale de cette nouvelle technologie par les utilisateurs. D'ailleurs, le traitement pourra également être permis s'il est *prévu par une loi*[10] ou lorsque le responsable du traitement peut faire valoir un

---

[7] Article 1er §2 de la LVP.

[8] Articles 4 et 5 de la LVP.

[9] Article 5 a) de la LVP.

[10] Article 5, c) de la LVP.

intérêt légitime qui prévaut sur les intérêts ou les droits et libertés fondamentaux de la personne concernée[11], en veillant notamment à ce que la dignité humaine de l'individu ne soit pas compromise.

24. La Commission souligne qu'un *consentement valable* est un consentement libre, spécifique et informé[12]. Un consentement libre implique entre autres qu'un système alternatif soit proposé à la personne concernée, lequel doit être équivalent et ne peut impliquer aucune sanction pour la personne concernée. Dans le secteur de la distribution[13] par exemple, le client devrait donner explicitement son consentement (opt-in) au commerçant pour qu'un tag sur un produit reste opérationnel après son achat. Si le client le souhaite, le commerçant doit dans ce cas procéder à la désactivation ou à l'élimination du tag, et ceci, sans coûts pour le consommateur. Le consommateur devrait également pouvoir vérifier si cette désactivation ou cette élimination a effectivement été effectuée.

25. L'attention doit également être attirée sur le fait que l'obtention d'un *consentement* ne justifie pas de traitement disproportionné. Le responsable du traitement doit veiller à la proportionnalité du traitement envisagé : l'intérêt général ou légitime du responsable du traitement doit être confronté au droit à la protection de la vie privée des personnes concernées. Une analyse de risque est dès lors recommandée avant de procéder à l'acquisition d'un tel système, en devant notamment comparer le système RFID envisagé avec les autres systèmes de traitement des données qui existent sur le marché.

26. Lorsque l'on invoque un *intérêt légitime*, il faut enfin faire remarquer que l'objectif pour lequel les données à caractère personnel sont traitées par exemple par un commerçant ne peut pas raisonnablement être réalisé d'une autre manière moins désavantageuse pour la personne concernée. Si un commerçant propose par exemple une carte client pourvue d'une puce RFID, le client doit pouvoir avoir le choix entre une carte anonyme (sans données à caractère personnel et qui n'est pas liée à une personne déterminée par le biais d'un fichier de données ou des informations de paiement) et une carte client contenant des données à caractère personnel.

---

[11] Article 5, f) de la LVP.

[12] Voir la définition du consentement de l'article 1er §8 de la LVP.

[13] Voir la Recommandation de la Commission européenne 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*, points 9-14.

B. Communication d'informations aux personnes concernées

27. A chaque traitement de données, les personnes doivent être informées des finalités du traitement, de l'identité du responsable du traitement et de ses destinataires (ou catégories de destinataires) des données, ainsi que de l'existence d'un droit d'accès et de rectification[14]. Dans le cas de la RFID, cette obligation d'information revêt une importance extrême étant donné la possibilité de traiter des données "invisibles" en utilisant des tags.

28. Chaque application RFID doit être accompagnée d'une politique en matière de vie privée compréhensible, qui devrait contenir au moins les éléments suivants[15] :

- identité et adresse du responsable du traitement ;
- but du traitement ;
- les données traitées, et plus particulièrement si des données à caractère personnel sont traitées, et si la localisation des tags sera ou non suivie ;
- une synthèse de l'évaluation d'impact sur la vie privée et la protection des données à caractère personnel (voir plus loin point 32) ;
- les risques potentiels en matière de respect de la vie privée concernant l'utilisation des tags dans l'application et les mesures que peuvent prendre les personnes concernées pour limiter ces risques.

29. Un autre élément de l'obligation d'information concerne la déclaration. En cas de traitement automatisé de données à caractère personnel, il faut en principe faire une déclaration préalable auprès de la Commission. L'article 55 de l'Arrêté royal *portant exécution de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel* prévoit une exception pour les traitements visant exclusivement la gestion de la clientèle (cartes client du magasin). Cette exception doit toutefois être interprétée de manière limitative. Si, par exemple, le fichier clients est utilisé pour établir des "profils d'utilisateurs", cette fonction ne tombe plus dans le champ de la simple gestion de la clientèle et doit donc faire l'objet d'une déclaration auprès de la Commission.

C. Durée de conservation des données

30. Les données à caractère personnel obtenues par le biais d'une application RFID et les données supplémentaires qui sont le résultat des conditions de la collecte ne devraient pas

[14] Article 9 de la LVP.

[15] Voir la recommandation de la Commission européenne du 12 mai 2009, op. cit., points 7-8.

être conservées plus longtemps que le temps nécessaire pour la réalisation de la finalité visée[16].

31. C'est ainsi par exemple que les tags sur un produit en magasin (destinés à la gestion des stocks) peuvent être désactivés par le client à son achat (cf. plus haut, point 24), si c'est possible pour le produit spécifique.

D. Mesures de sécurité

32. Le responsable du traitement et, le cas échéant, son sous-traitant, doivent prendre les mesures de sécurité techniques et organisationnelles[17] nécessaires pour protéger l'application RFID – y compris le système dans lequel on traite le flux de données – et les données à caractère personnel traitées par son biais contre la destruction accidentelle ou non autorisée, contre la perte accidentelle ainsi que contre la modification, l'accès et tout autre traitement non autorisé de données à caractère personnel. A ce sujet, la Commission renvoie pour information aux normes de sécurité établies par elle dont l'application à un traitement de données à caractère personnel doit, selon la Commission, être évaluée au cas par cas[18].

33. La Commission recommande en outre aux responsables[19] :

- de faire un "privacy assessment" de l'impact de l'application RFID sur la vie privée et la protection des données à caractère personnel, et notamment répondre à la question de savoir si l'application peut être utilisée pour le "monitoring" d'une personne. Plus les risques en matière de vie privée d'une application donnée sont élevés, plus le niveau de l'évaluation doit l'être ;
- de désigner les responsables pour le suivi des évaluations et vérifier l'efficacité des mesures de sécurité techniques et organisationnelles; il est indispensable que le responsable du traitement suive étroitement les évolutions technologiques afin d'y adapter les mesures de sécurité qu'il prend[20] ;
- de mettre l'évaluation à la disposition des autorités de contrôle au moins six semaines avant la mise en service de l'application.

---

[16] Article 4, §1er, 5° de la LVP.

[17] Article 16 de la LVP.

[18] http://www.privacycommission.be/fr/static/pdf/mesures-de-r-f-rence-vs-01.pdf.

[19] Voir la recommandation de la Commission européenne du 12 mai 2009, op. cit., points 4-5.

[20] Article 16 de la LVP.

34. Conformément à l'article 15*bis* de la LVP, le responsable du traitement peut être tenu responsable des dommages qui pourraient être dus au non-respect ou à l'inefficacité des mesures de sécurité.

35. Enfin, un rôle important est dévolu au secteur[21] en ce qui concerne les mesures de sécurité et de respect de la vie privée. De par l'application de ce que l'on appelle le "security and privacy by design", il devient beaucoup plus simple pour le responsable du traitement de mettre en place un système conforme aux exigences en matière de protection de la vie privée. La Commission est bien sûr toujours prête à organiser une concertation avec le secteur à ce sujet pour avis.

Pour l'Administrateur e.c., Le Président,

(sé) Patrick Van Wouwe (sé) Willem Debeuckelaere

[21] Voir la recommandation de la Commission européenne du 12 mai 2009, op. cit., point 17.