



Recommandation n° 01/2010 du 17 mars 2010

Objet: recommandation relative aux principes de base à respecter dans le cadre de l'utilisation de la télébilletique par les sociétés publiques de transport en commun (A-2010-003)

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 30 ;

Vu le rapport de Monsieur Mertens de Wilmars;

Émet, le 17 mars 2010, la recommandation suivante:

I. Introduction

1. L'utilisation de la télébilletique par les sociétés publiques de transports en commun, ci-après nommées les **Sociétés**, est un phénomène qui commence à prendre de l'ampleur. En effet depuis 2008, la STIB, en Région bruxelloise, a rendu opérationnel son système MOBIB, et les autres sociétés, De Lijn, SNCB et TEC envisagent d'avoir recours à cette technique dans un avenir plus ou moins proche. Cette technique fait usage d'une puce RFID insérée dans une carte plastique au format de la carte d'identité électronique.
2. Qui plus est, une plate forme commune aux Sociétés vient d'être créée à savoir la s.a. Belgian Mobility Card, de telle sorte qu'avec une seule carte à puce, un usager pourra utiliser les services des quatre Sociétés.
3. Un système de télébilletique comporte trois éléments principaux :
 - Une base de données « Clientèle » dans laquelle sont enregistrées des données, en nombre variable, relatives aux personnes physiques ayant conclu un contrat commercial avec la Société, sous la forme de l'achat d'un ou plusieurs titres de transport.
 - Une base de données «Trajet» dans laquelle sont enregistrées au moins des données relatives aux validations d'un titre de transport à chaque trajet effectué par l'usager, et souvent, par extension, relatives à ce trajet.
 - Une carte à puce RFID permettant d'effectuer la validation et contenant au minimum les données permettant d'identifier le propriétaire de la carte à puce et de vérifier la validité du titre de transport utilisé.
4. Ces réservoirs de données font l'objet de traitements distincts liés chacun à des finalités distinctes, découlant de la mission d'intérêt public remplie par les Sociétés. De ces traitements découlent d'une part des délais de conservation des données plus ou moins longs en fonction de la finalité visée, et d'autre part le fait que ces données sont utilisées soit comme telles (c'est-à-dire personnalisées) soit après codification soit encore après anonymisation.
5. La présente recommandation d'initiative a pour objet d'énoncer un certain nombre de principes à respecter lors de l'élaboration et de la construction d'un système de télébilletique de manière à protéger suffisamment la vie privée des usagers sans mettre en péril l'intérêt légitime de la Société d'utiliser un tel système pour satisfaire de manière adéquate aux exigences de sa mission d'intérêt public.

II. Les principes à respecter par un système de télébillettique au regard de la loi vie privée

1) Application de la loi vie privée

6. L'instauration d'un système télébillettique fonctionnant au moyen d'une carte à puce RFID contenant des données personnelles ainsi que la mise sur pied des bases de données clientèle et trajet constituent des traitements de données à caractère personnel rentrant dans le champ d'application de la loi vie privée, ce qui implique le respect par le responsable du traitement de l'ensemble des principes qu'elle édicte.

7. Les données traitées par les Sociétés dans le cadre des trajets effectués constituent des données à caractère personnel dont le traitement est soumis à la loi vie privée.

2) Admissibilité du traitement

8. L'article 5 de la loi vie privée énonce les hypothèses dans lesquelles un traitement de données à caractère personnel peut être réalisé. La mise en œuvre d'un système télébillettique pourrait rentrer dans les hypothèses prévues aux articles 5, b), c) et e) car ce traitement serait nécessaire à l'exécution d'un contrat auquel la personne concernée est partie, nécessaire au respect d'une obligation à laquelle le responsable du traitement est soumis par ou en vertu d'une loi, d'un décret ou d'une ordonnance et nécessaire à l'exécution d'une mission d'intérêt public dont est investi le responsable du traitement.

3) Voyager de manière anonyme

9. **À cet égard, la Commission est d'avis que les Sociétés ne peuvent pas traiter, directement ou indirectement, des données à caractère personnel qui permettrait de tracer le trajet des usagers sur base de leur titre de transport électronique.**

4) Principe de finalité

10. Le principe de finalité stipulé à l'article 4 de la loi vie privée, impose au responsable du traitement de ne collecter des données que pour une ou des finalités déterminées, explicites et légitimes et de ne traiter les données ainsi collectées que de manière compatible avec ces finalités.

11. Au vu de l'analyse des systèmes de télébilletique opérationnels, la Commission considère exclusivement comme étant raisonnablement attendues d'un système de télébilletique, composé des éléments définis plus haut, les finalités suivantes :

- **La gestion des titres de transport** : notamment le traitement des cas de perte ou de vol des titres de transport ;
- **La gestion des fraudes** : s'assurer que chaque usager a effectivement payé son trajet et a contrario détecter les usagers voyageant sans être porteur d'un titre de transport dûment validé ;
- **La gestion technique** : détecter les lecteurs de cartes qui présentent une anomalie ;
- **La gestion statistique** : d'après les informations recueillies par la Commission, celle-ci porte exclusivement sur deux aspects, à savoir :
 - l'historique des contrats souscrits par catégorie d'usagers ;
 - l'historique d'usage du transport public par catégorie d'usagers ;

12. Dans le cadre d'une coordination avec la base de données clientèle, viennent s'ajouter deux finalités à savoir :

- **La gestion de la clientèle** : gestion des comptes clients ayant contracté avec la Société ;
- **Le marketing direct** : l'information de la clientèle sur l'évolution des produits et des offres particulières proposées par la Société¹.

5) La durée de conservation

13. L'article 4, § 1, 5° de la loi vie privée impose une obligation de limitation quant à la durée de conservation des données qui ne peut être plus longue que le temps nécessaire à la réalisation des finalités pour lesquelles elles ont été obtenues.

¹ La Commission attire l'attention des Sociétés sur la recommandation qu'elle a adoptée le 14 octobre 2009 concernant le marketing direct et la protection des données à caractère personnel (n° 04/2009) et les principes à respecter qu'elle y édicte.

14. Au regard des seules finalités raisonnablement admises par la Commission dans le cadre de l'exploitation d'un système de télébilletique, celle-ci préconise les délais de conservation des données nécessaires à l'exercice de ces finalités comme suit :

- **La gestion des titres de transport** : les données enregistrées pour l'exercice de cette finalité ne peuvent être conservées plus de 6 mois au-delà de la date d'expiration du dernier contrat conclu par l'utilisateur. La Commission estime raisonnable le délai de 6 mois laissé à l'utilisateur pour porter réclamation quant à l'utilisation d'un titre de transport quel qu'il soit².
- **La gestion des fraudes** : les données enregistrées pour l'exercice de cette finalité ne peuvent être conservées au-delà du délai nécessaire à la constatation de la fraude. Au-delà de ce délai les données à conserver doivent faire l'objet d'un réceptacle particulier dans lequel les données pourraient être conservées aussi longtemps que le nécessite la procédure entamée à l'issue d'une fraude avérée.
- **La gestion technique** : les données enregistrées pour l'exercice de cette finalité ne peuvent être conservées au-delà du délai nécessaire à la constatation de l'incident technique. Au-delà de ce délai, les données à conserver doivent faire l'objet d'un réceptacle particulier dans lequel les données pourraient être conservées aussi longtemps que le nécessite la procédure entamée à l'issue d'une anomalie confirmée.
- **La gestion statistique** : dans le cadre de cette finalité, les données ne peuvent en aucun cas être conservées en l'état. Elles doivent être conservées sous une forme effectivement anonymisée. Le délai de conservation des données brutes (donc encore personnalisées) ne sera pas supérieur au délai nécessaire pour effectuer la(les) segmentation(s) désirée(s). Le délai de conservation des données anonymisées n'étant quant à lui pas limité³.

² A moins qu'il soit nécessaire de se conformer aux obligations prévues par la loi sur les pratiques commerciales.

³ En vertu de l'arrêté royal du 13 février 2001 portant exécution de la loi vie privée doivent être considérées comme :

- des données à caractère personnel codées : les données à caractère personnel qui ne peuvent être mises en relation avec une personne identifiée ou identifiable que par l'intermédiaire d'un code (article 1, 3°);
- des données anonymes : les données qui ne peuvent être mises en relation avec une personne identifiée ou identifiable et qui ne sont donc pas des données à caractère personnel (article 1, 5°).

15. Dans le cas où une coordination entre les bases de données intervient, le délai de conservation des données pourrait être défini comme suit :

- **La gestion de la clientèle** : les données enregistrées pour l'exercice de cette finalité ne peuvent être conservées plus de 12 mois au-delà de la date de l'expiration du dernier contrat conclu par un usager pour autant qu'il ait restitué la carte à puce servant de support à l'enregistrement des contrats.
- **Le marketing direct** : les données enregistrées pour l'exercice de cette finalité ne peuvent être conservées au-delà de la date d'expiration du dernier contrat conclu par l'usager.

6) Principe de proportionnalité

16. Le principe de proportionnalité stipulé à l'article 4 de la loi vie privée, impose au responsable du traitement de ne collecter, pour réaliser la ou les finalités poursuivies, que des données à caractère personnel adéquates, pertinentes et non excessives. Dans le choix des modalités de traitement permettant d'atteindre la finalité poursuivie, le responsable du traitement devrait également veiller à opter pour celles qui sont les moins attentatoires à la vie privée des personnes concernées. Une ingérence dans le droit à la protection des données des personnes concernées doit en effet être proportionnée au regard des finalités du traitement pour le responsable du traitement.

17. Les délais de conservation ayant été définis ci-dessus, les données pouvant être conservées peuvent être définies comme suit :

- **La gestion des titres de transport** : les données de la gestion de la clientèle et les données nécessaires pour caractériser les contrats en vigueur ;
- **La gestion des fraudes** : les données d'identification du présumé fraudeur et les données de trajet permettant d'établir la fraude ;
- **La gestion technique** : les données d'identification des clients lésés, des contrats mis en cause et les données relative au trajet liées à l'incident technique ;
- **La gestion statistique** : toutes les données de clientèle et de trajet pour autant qu'elles soient anonymisées ;

- **La carte RFID :**

- les données visibles autorisées sont limitées à :
 - la photo du titulaire de la carte ;
 - le numéro de client ;
 - le numéro technique de la carte ;
 - le nom, le prénom et la date de naissance du titulaire de la carte.
- Les données non visibles, présentent sur la puce de la carte, autorisées sont :
 - les données personnelles du client nécessaires à son identification (lors de l'achat de titre de transport ou lors d'un contrôle) ;
 - les dernières validations nécessaires à effectuer un contrôle cohérent et efficace ;
 - les contrats achetés et toujours valides.

18. En cas de mise en relation entre la base de données trajet et la base de données clientèle, les données pouvant être conservées peuvent être les suivantes :

- **La gestion de la clientèle :** les données personnelles du client auxquelles sont associées un numéro de client ;
- **Le marketing direct :** les coordonnées du client.

7) Principe de la sécurité de traitement

19. La Commission souhaite souligner l'importance du respect du principe de sécurisation des traitements de données à caractère personnel, prévu à l'article 16 de la loi vie privée, qui impose au responsable du traitement de prendre des mesures techniques et organisationnelles adéquates pour protéger les données à caractère personnel qu'il traite et se prémunir contre les détournements de finalité. Le caractère adéquat de ces mesures de sécurité dépend, d'une part, de l'état de la technique et des frais engendrés et d'autre part, de la nature des données à protéger et des risques potentiels. Les Sociétés doivent tenir compte des «mesures de référence en matière de sécurité applicables à tout traitement de données à caractère personnel» qui sont publiées sur le site web de la Commission⁴.

⁴ <http://www.privacycommission.be/fr/static/pdf/mesures-de-r-f-rence-vs-01.pdf>

20. Si les Sociétés font appel à un sous-traitant, elles devront également respecter les dispositions relatives à la conclusion d'un contrat de sous-traitance en bonne et due forme (article 16 de la loi vie privée). Il convient dans ce cadre de fixer la responsabilité du sous-traitant et de convenir explicitement que le sous-traitant et les personnes agissant sous son autorité ne peuvent agir, dans le cadre de la mission spécifique de sous-traitance, que sur instruction du responsable du traitement.

8) Information des personnes concernées

21. L'article 9 de la loi vie privée impose à tout responsable de traitement d'informer les personnes dont les données sont traitées quant aux finalités de traitement, à l'identité du responsable du traitement et des destinataires (ou catégories de destinataires) des données ainsi qu'à l'existence du droit d'accès et de rectification de la personne concernée (voir point 22 de la présente recommandation).

9) Droit d'accès des personnes concernées (droit de consultation)

22. En vertu des articles 10 et 12 de la loi vie privée, les personnes concernées disposent d'un droit d'accès aux données à caractère personnel les concernant qui ont fait l'objet d'un enregistrement, le droit de faire rectifier les données inexactes qui les concernent ainsi que le droit d'obtenir la suppression des données qui, compte tenu des finalités du traitement, sont inexactes ou dont l'enregistrement, la communication ou la conservation sont interdits par la loi, ou qui ont été conservées au-delà du délai raisonnable.

23. La Commission souhaite également que les Sociétés précisent (dans les conditions générales qui sont remises au client par exemple) le point de contact (un numéro de téléphone et/ou une adresse email spécifique doit être précisé au minimum) auprès duquel les personnes concernées peuvent faire valoir les droits précités.

III. Conclusions

24. La Commission estime que les présents principes représentent les lignes directrices à respecter par toute Société lors de l'élaboration et de la mise en place d'un système de télébilletique.

Pour l'Administrateur e.c.,

Le Président,

(sé) Patrick Van Wouwe

(sé) Willem Debeuckelaere