Direction Générale – Espaces, Services et Vente

15 Octobre 2004	
Diffusion :	Tous départements Toutes Délégations Toutes Missions

INSTRUCTION GENERALE N°503

CONFIDENTIALITE DES INFORMATIONS UTILISEES PAR LA CARTE ET LES SYSTEMES TELEBILLETTIQUES ET RELATIVES AUX DEPLACEMENTS DES PERSONNES

MARS 2007

Le Directeur Général Adjoint

Signé sur l'original

Philippe MARTIN

Suivi des modifications

Date	N° IG	Modification/Origine
1 mars 2007	IG503	Mise à jour de l'annexe n°1
30 novembre 2011	IG503	Mise à jour de l'annexe n°1

Documents de référence

Référence	Date	Intitulé
CNIL Délibération n° 03-038	16 septembre 2003	Délibération portant adoption d'une recommandation relative à la collecte et au traitement d'informations nominatives par les sociétés de transports collectifs dans le cadre d'applications billettiques
CNIL Délibération n° 04-020	8 avril 2004	Délibération portant avis sur un traitement de la Régie Autonome des Transports Parisiens ayant pour finalité l'exploitation des données de validations des passes NAVIGO

Table des matières

1 Contexte général de la télébillettique

Les traitements de la carte télébillettique entraînent au moment de la validation en entrée, en correspondance ou en sortie, l'inscription sur la carte de la date, de l'heure et du lieu de la validation et la collecte dans les systèmes centraux, du numéro de la carte, de la date, de l'heure et du lieu de la validation.

Le groupe d'informations -numéro de la carte, date, heure, lieu de la validation- présente un caractère d'information indirectement nominative, et en conséquence confidentielle.

La CNIL a publié le 16 septembre 2003 une délibération n°03-038 relative aux traitements dans le cadre des applications billettiques dans laquelle elle souligne que du fait de cette collecte, "*les déplacements des personnes utilisant ces cartes peuvent être reconstitués et ne sont plus anonymes, ce qui est de nature à porter atteinte tant à la liberté, fondamentale et constitutionnelle, d'aller et venir, qu'au droit à la vie privée qui constitue également un principe de valeur constitutionnelle*."

La RATP a mis en place des dispositions techniques et des procédures pour empêcher la reconstitution des déplacements de voyageurs identifiés.

Les traitements des données de validation réalisés par la RATP ont reçu un avis favorable de la CNIL.

2 Protection des données de déplacement contenues dans la carte

Pour permettre le fonctionnement des programmes informatiques chargés de la validation du contrat de transport, la carte mémorise les trois dernières validations effectuées.

Les matériels permettant de lire ces validations sont des matériels destinés au seul usage des personnels d'exploitation en relation avec les voyageurs :

- les terminaux points de vente,
- les terminaux portatifs de contrôle.

2.1 Cadre général pour la communication des informations portées par la carte à la suite d'une demande du titulaire

La loi donne au titulaire le droit d'accéder aux informations portées par les passes NAVIGO personnalisés. Ce droit d'accès s'exerce auprès du Département Commercial, Gestion des Titres Longs, 54, quai de la Rapée, 75599 PARIS Cedex 12, après justification préalable de l'identité du demandeur conformément à la Notice Technique D n°4 du 16 novembre 1981.

Le droit d'accès ne peut pas être exercé pour des passes "anonymes", même s'il s'agit de cartes "déclaratives" (carte personnalisée par le titulaire lui même).

2.2 Cas particulier de la communication directe par un agent d'exploitation à un voyageur des données portées par la carte

Les seules informations qui peuvent être communiquées par un agent d'exploitation à un voyageur sont celles permettant d'expliquer un refus de validation ou de justifier une verbalisation, c'est à dire en général les informations concernant la dernière validation.

Dans les autres cas, le voyageur doit être invité à exercer son droit d'accès comme prévu au paragraphe 2.1.

Cette protection ne s'applique pas aux informations relatives aux contrats portés par la carte et à leur validité temporelle ou géographique qui peuvent être communiquées sans restriction au voyageur.

Les autres agents de l'entreprise ne sont pas autorisés à communiquer directement les informations portées sur la carte à un voyageur ou à un tiers.

3 Protection des données mémorisées dans les systèmes centraux

3.1 Cadre général

Les données collectées par les systèmes centraux sont

- transmises au système de surveillance de la fraude technologique,
- réparties dans des fichiers cloisonnés pour le suivi du fonctionnement des cartes et des valideurs et pour la constitution des états statistiques de trafic.

Les dispositions techniques mises en œuvre ne permettent pas la reconstitution des déplacements d'un voyageur. Toute tentative de contournement de ces dispositions constitue un délit (Code Pénal Art 226-16 et suivants).

3.2 Exercice du droit d'accès par un client

La loi donne au titulaire d'un passe NAVIGO personnalisé le droit d'accéder aux informations contenues dans les systèmes centraux. L'exercice de ce droit d'accès s'exerce dans les mêmes conditions que celles prévues au paragraphe 2-1. Compte tenu des dispositions techniques mises en œuvre, seul le nombre d'utilisations d'un passe aux cours des jours précédents pourra matériellement être communiqué au voyageur.

4 Cas des réquisitions judiciaires

4.1 Demande d'accès aux données portées par le passe NAVIGO

Les officiers de police judiciaire (OPJ) peuvent demander l'accès aux données portées par le passe NAVIGO après avoir justifié de leur qualité et remis une réquisition judiciaire.

L'agent RATP requis procède immédiatement à la lecture du passe au TPV, ou informe immédiatement l'OPJ du nom de la personne à requérir afin qu'elle procède à la lecture du passe.

L'agent RATP qui effectue la lecture du passe au TPV, procède à l'impression du contenu du passe,

- communique l'information à l'OPJ sous la forme d'un rapport, auquel il annexe le ticket imprimé,
- transmet une copie de ce rapport accompagnée de la réquisition judiciaire à sa hiérarchie et au Responsable Sécurité des Systèmes d'Information de la RATP (RSSI).

En l'absence de réquisition judiciaire, la personne interrogée doit indiquer qu'il n'est pas possible de répondre à la demande.

4.2 Demande d'accès aux données contenues dans les systèmes

Les officiers de police judiciaire (OPJ) peuvent demander l'accès aux données de validation contenues dans les systèmes après avoir justifié de leur qualité et remis une réquisition judiciaire en s'adressant à l'IPEX. En l'absence de réquisition judiciaire, l'IPEX doit indiquer qu'il n'est pas possible de répondre à la demande.

4.2.1 Accès aux validations effectuées par un voyageur

Les mesures techniques mises en œuvre pour garantir l'anonymat des déplacements ne permettent pas de répondre à ce type de demande. L'IPEX informe immédiatement l'OPJ de cette situation.

4.2.2 Enregistrement des validations futures d'un voyageur

La réalisation de ce type d'enregistrement ne fait pas partie des finalités du système. L'IPEX transmet la réquisition aux personnes en charge de la sécurité des systèmes télébillettiques pour analyser la possibilité de répondre à la demande et procéder à la mise en œuvre éventuelle, communique à l'OPJ les coordonnées de la personne chargée de la réponse.

Si la demande est réalisable, l'agent RATP chargé de la réponse

- procède à la recherche d'information
- communique directement l'information à l'autorité judiciaire sous la forme d'un rapport écrit,
- transmet une copie de ce rapport écrit accompagnée de la réquisition judiciaire à sa hiérarchie et au Responsable Sécurité des Systèmes d'Information de la RATP (RSSI).

5 Cas des personnels techniques intervenant sur les systèmes et les cartes télébillettiques

Les personnels techniques intervenant sur les systèmes et les cartes télébillettiques au titre de l'ingénierie, de l'administration des systèmes ou de la maintenance sont susceptibles d'accéder à des données sensibles. Ils sont soumis à une obligation de confidentialité.

Le responsable d'entité doit leur faire signer un engagement de confidentialité conforme au modèle de l'annexe n°2 et leur communiquer contre émargement la présente Instruction Générale.

6 Annexe n°1 à l'IG N° 503 - Liste des personnes habilitées à demander l'accès aux informations contenues dans les systèmes centraux

Nom	Fonction	Département
Jean Pierre TRANG	Chargé de la surveillance de la fraude technologique	CML/D1R/SI
Patrick DOCQUIER	Responsable Départemental de la Sécurité des Systèmes d'Information	CML/DIR/SI
François LEJOYEUX	Responsable Sécurité du Système d'Information Billettique	CML/DIR/SI
François LACROIX	Assistant au responsable Sécurité du Système d'Information Billettique	CML/DIR/SI
Julien TESLER	Assistant au responsable Sécurité du Système d'Information Billettique	CML/DIR/SI
Gwenolé DENIEUL	Assistant au responsable Sécurité du Système d'Information Billettique	CML/DIR/SI
Medhi AIT HAMMOU	Responsable de la Sécurité des Systèmes d'Information	CGS
Jean CAIRE	Adjoint du Responsable de la Sécurité des Systèmes d'Information	CGS

7 Annexe n°2 à l'IG n°503 – Modèle d'engagement de confidentialité

DONNEES DE VALIDATION DU PASSE NAVIGO

CONFIDENTIALITE DES INFORMATIONS

Dans le cadre du traitement des données de validation du Passe Navigo, il convient de rappeler aux utilisateurs du système les règles concernant la protection des données personnelles telles qu'elles figurent dans la loi relative à l'informatique, aux fichiers et aux libertés (voir les articles 1 et 29 rappelés ci-dessous, complétés par l'article 226-22 du code pénal)

Certaines données contenues dans les systèmes de télébillettique sont relatives au déplacement des personnes et relèvent, à ce titre, de leur vie privée. La RATP s'est engagée à prendre toutes mesures utiles afin de préserver la confidentialité de ces informations et, notamment, d'empêcher qu'elles soient communiquées à des tiers non autorisés.

En conséquence, l'accès à ces données est réservé aux utilisateurs dûment autorisés. Dans les cas où l'accès est protégé par un mot de passe personnel, l'autorisation est strictement personnelle : l'utilisateur s'interdit de divulguer son mot de passe. Il est responsable de l'utilisation qui peut en être faite. Dans les cas où l'accès est protégé par un mot de passe partagé, l'utilisateur s'interdit de le divulguer à des personnes non autorisées. Dans tous les cas il s'interdit, sous peine de commettre un délit, de communiquer les informations auxquelles il a accès aux tiers qui n'ont pas qualité pour les recevoir.

Loi 78-17 du 6 janvier 1978 - Article 1 : " L'informatique doit être au service de chaque citoyen. Son développement doit s'opérer dans le cadre de la coopération internationale. Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques. "

Loi 78-17 du 6 janvier 1978 - Article 34, alinéa 1 : " Le responsable du traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès "

Code Pénal - Article 226-22 : "Le fait, par toute personne qui a recueilli, à l'occasion de leur enregistrement, de leur classement, de leur transmission ou d'une autre forme de traitement, des données à caractère personnel dont la divulgation aurait pour effet de porter atteinte à la considération de l'intéressé ou à l'intimité de sa vie privée, de porter, sans autorisation de l'intéressé, ces données à la connaissance d'un tiers qui n'a pas qualité pour les recevoir est puni de cinq ans d'emprisonnement et de 300 000 Euros d'amende.
La divulgation prévue à l'alinéa précédent est punie de trois ans d'emprisonnement et de 100 000 Euros d'amende lorsqu'elle a été commise par imprudence ou négligence.
Dans les cas prévus aux deux alinéas précédents, la poursuite ne peut être exercée que sur plainte de la victime, de son représentant légal ou de ses ayants droit."

L'utilisateur soussigné reconnaît avoir pris connaissance des règles contenues dans la présente note et dans l'Instruction Générale n° 503 et s'engage à s'y conformer strictement.

PRENOM	NOM	MATRICULE	UNITE	DATE	SIGNATURE