URBA 2000

L'autorisation unique de la CNIL pour la mise en œuvre de traitements automatisés de données à caractère personnel dans la gestion des systèmes billettiques

Comité de pilotage de la PREDIM – 14 octobre 2008

I - PRINCIPES

Textes de référence et définitions

Textes

France	Loi n°78-17 du 6 janvier **1978** dite loi informatique et libertés. Elle créé une autorité indépendante, la "Commission Informatique et Liberté", CNIL, *chargée "de veiller à ce que l'informatique soit au service du citoyen et qu'elle ne porte atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée ni aux libertés individuelles et publiques."*
Europe	Directive 95-46 CE du Parlement et du Conseil du 24 octobre **1995** relative A la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.
Europe	Charte des droits fondamentaux de l'Union Européenne publiée le 18 décembre **2000**
International	Convention du 28 janvier **2001** du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel
France	Loi n°2004-801 du 6 Août **2004** modifiant la loi du 6 janvier 1978 et transposant la Directive 95-46 CE

Définitions

Donnée à caractère personnel

Constitue une ***donnée à caractère personnel*** toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à

un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres (nom et prénom, date de naissance, éléments biométriques, empreinte digitale, ADN...)

Constitue un ***traitement de données à caractère personnel*** toute opération ou tout ensemble d'opérations portant sur de telles données, quel que soit le procédé utilisé.

Constitue ***un fichier de données à caractère personnel*** tout ensemble structuré et stable de données à caractère personnel accessibles selon des critères déterminés.

Les données doivent être collectées pour ***des finalités*** déterminées, explicites et légitimes et ne doivent pas être excessives au regard de ces finalités (les informations exploitées dans un fichier doivent être cohérentes par rapport à son objectif ; elles ne doivent pas être réutilisées de manière incompatible avec la finalité pour laquelle elles ont été collectées).

Les informations sont conservées sous une forme permettant l'identification des personnes concernées pendant une durée qui n'excède pas la durée nécessaire aux finalités pour lesquelles elles sont collectées et traitées. Au-delà de cette durée les données à caractère personnel doivent faire l'objet d'un **procédé d'anonymisation** reconnu par la CNIL.

Les relations des gestionnaires de traitements de données à caractère personnel avec la CNIL

Le régime institué par la loi 1978 soumettait à une autorisation préalable les fichiers contenant des données à caractère personnels créés et gérés par les autorités publiques ou les gestionnaires de services publics ; les personnes privées n'étaient, quant à elles, soumises qu'à une déclaration préalable.

Depuis 2004, la philosophie de la loi "Informatique et Libertés" dans sa nouvelle rédaction est de soumettre à autorisation préalable de la CNIL les traitements présentant des risques pour les droits des personnes ; le régime de formalités ne dépend plus seulement d'un critère organique, c'est à dire l'appartenance du responsable de traitement au secteur public ou au secteur privé, mais d'un critère matériel, à savoir le caractère sensible du traitement. Huit catégories de traitements sont soumises à autorisation préalable de la CNIL.

II - PRECEDENT
La recommandation n°03-038 du 16 septembre 2003

S'agissant de la billettique, la CNIL a été amenée à émettre une première recommandation suite à la demande d'autorisation de la RATP concernant le PASSE NAVIGO en 2003.

La CNIL constate que l'utilisation de cartes nominatives entraîne la collecte des trajets effectués par le titulaire de la carte, à l'occasion de la validation. En effet, les date, heure, et lieu de validation ou de correspondance et le numéro de la carte sont mémorisés. Or le numéro de la carte est indirectement nominatif car il rend possible l'identification de son titulaire dont les coordonnées figurent dans le fichier clientèle.

Ainsi, les déplacements effectués en utilisant la carte ne sont plus anonymes, ils sont traçables et cette ***traçabilité des déplacements*** est de nature à porter atteinte à deux libertés fondamentales : ***la liberté d'aller et venir et le respect de la vie privée*.**

Conformément aux principes rappelés ci-dessus, la recommandation de la CNIL porte sur l'identification des finalités du traitement des données à caractère personnel, l'anonymisation des données, la durée de conservation des données dans le cadre de la lutte contre la

fraude fixée à deux jours ou, si la fraude est avérée, pendant le temps d'instruction de l'affaire par les autorités judiciaires.

Elle affirme également qu'il est hautement souhaitable que soit maintenue la possibilité de circuler de manière anonyme, au moyen d'un titre billettique ou autre. En d'autres termes, les clients abonnés du service de transport public doivent être en mesure de choisir entre un Passe nominatif et un Passe anonyme. De plus, dans un avis du 8 avril 2004, la Commission avait estimé que le choix d'un Passe anonyme ne devait pas engendrer de surcoût par rapport au choix du Passe nominatif.

Cette dernière recommandation a été suivie sur le principe. Elle a été à l'origine de la création, en Ile de France, du PASS NAVIGO DECOUVERTE en septembre 2007, dont le prix est légèrement supérieur à celui du PASS NAVIGO nominatif.

Sur la base des principes exprimés par cette recommandation, la CNIL a été appelée à plusieurs reprises à formuler un avis sur d'autres systèmes billettiques mis en œuvre sur le territoire national.

III - DROIT EN VIGUEUR
L'autorisation unique AU 015

La notion d'autorisation unique

Le régime de l'autorisation unique est prévu par l'article 26-3 de la loi informatique et libertés de janvier 1978 modifiée en 2004. Elle décrit les règles applicables aux fichiers et traitement de données qui visent une même finalité et des catégories de données et de destinataires identiques. Lorsqu'une telle autorisation existe, il n'est plus nécessaire d'effectuer les formalités de déclaration ou d'autorisation préalable si l'on s'y conforme ; un formulaire de déclaration de conformité suffit. Dans le cas contraire, si l'on y déroge totalement ou partiellement, l'autorisation préalable est de nouveau requise.

Le 3 juin 2008 la CNIL a pris une décision d'autorisation unique n° AU-015 concernant la mise en œuvre des traitements automatisés de données à caractère personnel dans la gestion des applications billettiques par les autorités organisatrices et les exploitants de transport. Cette autorisation a été publiée au Journal officiel du 2 juillet 2008.

Le dispositif

La préparation de cette autorisation a été relativement longue. Sa dernière version provisoire a donné lieu à commentaires de la part des acteurs concernés du transport public consultés par la Commission. .Ceux qui nous sont connus, permettent de situer les termes du débat de ces derniers avec la CNIL.

Les fondements de l'autorisation préalable

Outre la question de la traçabilité des déplacements, la CNIL appuie la légitimité de son intervention sur l'article 25-I-4 de la loi informatique et libertés qui soumet à autorisation préalable *« les traitements automatisés susceptibles, du fait de leur nature, de leur portée ou de leurs finalités, d'exclure des personnes du bénéfice d'un droit, d'une prestation ou d'un contrat en l'absence de toute disposition législative ou réglementaire »*

Son analyse diffère de celles des transporteurs qui soutiennent que l'application de l'article 25-1-4 n'est pas avérée dans le cas des impayés car la résiliation du contrat entre le client et le transporteur résulte du contrat de transport, contrat synallagmatique, qui fait naître des obligations réciproques et interdépendantes entre les cocontractants (le paiement étant la contrepartie du droit à voyager). Il n'y a donc pas d'exclusion unilatérale d'une partie à l'encontre de l'autre. Par ailleurs, le voyageur dispose toujours de la faculté d'utiliser des tickets à l'unité ou d'autres produits tarifaires. .

La CNIL a estimé que cette argumentation qui repose sur le droit des contrats régi par le code civil, n'est pas incompatible avec l'application de l'article 25-1-4 de la loi informatique et libertés qui vise les traitements automatisés susceptibles d'exclure des personnes du bénéfice d'un contrat ou d'une prestation malgré l'existence d'alternatives permettant de continuer, par d'autres moyens tarifaires, d'utiliser le service public des transports publics.

Les finalités de l'utilisation et du traitement de données à caractère personnel

Les finalités décrites dans l'autorisation sont plus clairement décrites qu'en 2003 et paraissent rejoindre d'assez près les souhaits des autorités et des professionnels :

- Gestion, délivrance et utilisation des titres de transport
- Gestion et suivi des relations commerciales
- Gestion de la fraude
- Analyses statistiques
- Mesures de la qualité du fonctionnement des services

Les données à caractère personnel traitées

Les transporteurs avaient fait observer la difficulté de faire référence à une liste exhaustive des données, compte tenu des évolutions tarifaires et technologiques. Il était préconisé de regrouper ces données en cinq catégories fonctionnelles génériques sans nécessairement dresser une liste précise des contenus de ces catégories :

- Données de personnalisation
- Données de vente et d'après vente
- Données de distribution
- Données de validation et de contrôle
- Données de sécurité.

La CNIL n'a pas suivi cette suggestion et a opéré une classification en trois catégories précisément décomposées. :

Une première catégorie vise les données relatives à la gestion, la délivrance et à l'utilisation des titres de transport billettiques, aux analyses statistiques, à la mesure de la qualité du fonctionnement des services, à la gestion de la fraude et à la détection de la fraude technologique. On y retrouve :

- les données de personnalisation (état civil, données relatives au paiement, données socio-professionnelles, carte d'identité en cas de paiement à distance, photo, justificatif de domicile…) ;
- les données de vente (le numéro de client, l'historique client, le type d'abonnement) ;
- les données d'après vente (les dates de début et de fin de validité de la carte, numéro de carte) ;
- les données de validation (date, heure, lieu de la validation)

- les données de contrôle (le motif de l'inscription sur un fichier d'exclusion d'après une liste fermée).

La seconde catégorie vise les données nécessaires à la gestion des tarifs sociaux (titres de transports gratuits ou à tarif réduit) : scolarité ; handicap ; bénéfice d'une allocation sociale ; âge ; revenus ; famille nombreuse… Les transporteurs avaient fait observer qu'il serait utile de prendre en compte les données permettant de justifier de certaines réductions tarifaires actuelles ou à venir issues des politiques de mobilité durable. La CNIL utilise le terme « d'allocation sociale » qui est connoté et qui devra certainement faire l'objet d'une interprétation large pour qu'y soient incluses les réductions « citoyennes ».

La troisième catégorie concerne la gestion des impayés : outre les informations d'état civil et bancaires, le montant de l'impayé, le numéro du chèque ou de carte bancaire, la date du rejet, le motif sous la forme d'une liste fermée indiquant par exemple l'absence ou l'insuffisance de provision, ou le moyen de paiement invalide ; le nombre d'avertissements avant suspension de l'abonnement, les données relatives au règlement des sommes dues. Cette énumération semble prendre en compte les souhaits formulés par les transporteurs.

Les restrictions d'usage et de conservation des données

- Le nombre d'événements de validation enregistrés dans la carte doit être limité à quatre et peut être étendu à six pour des besoins d'interopérabilité. Sur ce point la CNIL a évolué par rapport à sa position de 2003 où elle notait : *« le nombre d'événements de validation enregistrés dans la carte, qui varie actuellement entre deux et six, devrait, à l'occasion du passage à la prochaine génération de carte, être limité à quatre ».*

- Les données de validation ne peuvent être collectées et associées aux données d'identification de l'abonné (par exemple son numéro de carte) que dans le cadre du traitement de la détection de la fraude. Dans ce cas, la CNIL reprend la recommandation de 2003 et prévoit une possibilité de conservation pendant 48 heures.

- Ces données, non associées aux numéros de carte ou à quelque autre moyen d'identification directe des abonnés, peuvent être collectées à des fins statistiques. Au titre de la gestion de la clientèle, les informations permettant d'identifier l'utilisateur peuvent être associées à la date et l'heure de validation, sous réserve que les informations relatives au lieu soient supprimées dans la limite d'un mois au maximum

  Illustration : la carte KORRIGO

  L'avertissement publié par les gestionnaires de la carte KORRIGO en usage dans l'agglomération de Rennes paraît répondre à cette recommandation. En effet, il y est en effet fait état de trois bases de données distinctes :

  - *La première contient les numéros de carte et les heures de validation ;*
  - *La seconde contient le lieu et le jour de validation*
  - *La troisième est la base de données clients proprement dite*

  .

Il n'est pas possible de faire un rapprochement entre les deux premières bases car il n'y a plus de dénominateur commun (le numéro unique de la carte du client).

La seconde base de données (lieu et jour de la validation) est utilisée pour les statistiques ; la première base de données (n° de carte et heure) est utilisée pour l'après-vente, notamment en cas de perte ou de vol).

La durée de conservation des données

a) L'ensemble des données clients est conservé pendant la durée de la relation contractuelle, et à l'issue de celle-ci pendant deux ans à des fins commerciales et statistiques pour les clients et prospects. Le terme de « relation contractuelle » renvoie à la relation entre l'opérateur de transport et son client. L'observation des transporteurs tendant à ce que soit prise en compte l'obligation de conserver, pendant toute la durée de la délégation les liant à l'autorité organisatrice, tous les abonnements souscrits par les voyageurs, n'est pas prise en compte.

b) Dans le cadre des traitements mis en oeuvre, les données de validation font l'objet d'une anonymisation à bref délai. Cette anonymisation est réalisée soit par la suppression complète du numéro de carte, soit par la suppression conjointe de la date, de l'heure et du lieu de passage, soit encore par l'application au numéro de carte d'un algorithme cryptographique de « hachage » public réputé fort.

Aujourd'hui toutes les applications billettiques font appel à la cryptographie pour anonymiser les données.

Information des personnes

a) l'autorisation unique prévoit :

« Les personnes susceptibles d'être inscrites dans le traitement de gestion des impayés doivent en être informées :
– lors de la conclusion du contrat d'abonnement ;
– préalablement à l'inscription dans le fichier des impayés et de la mise en opposition du titre de transport.

Le cas échéant, si un délai est accordé lors d'une mise en demeure de payer, le responsable de traitement doit mentionner sur les lettres de relance le délai dont dispose la personne concernée pour régulariser sa situation, ainsi que les conséquences de la mise en opposition de son passe. »

b) Dans la mesure où une telle obligation serait lourde et complexe à mettre en œuvre, les transporteurs avaient souhaité que l'information préalable à l'inscription dans le fichier des impayés ne soit pas maintenue. Ils n'ont pas été entendus par la Commission sur ce point.

IV - APPLICATION ET PERSPECTIVES

1) Le régime de l'autorisation unique est de nature à simplifier la mise en place des systèmes de billettique intermodale puisqu'il trace un cadre clair et qu'il suffira désormais au gestionnaire de fichiers contenant des données à caractère personnel de se déclarer conforme à l'autorisation unique.

On doit cependant faire observer que les discussions qui ont abouti à l'autorisation unique se sont appuyées sur des systèmes de billettique gérant de manière exclusive (ou quasi exclusive) des abonnements bénéficiant de tarifs personnalisés (et plus particulièrement la carte NAVIGO d'Ile de France).

On doit aussi rappeler que la CNIL, à plusieurs reprises, a demandé que l'offre billettique ne soit pas réduite à une carte nominative et qu'il soit offert aux usagers du transport la possibilité, sans surcoût, de disposer d'une carte anonyme. Cette demande a été à l'origine de la création du PASSE NAVIGO DECOUVERTE. Cette carte ne comporte aucune mention identitaire (et ne permet pas de tracer les déplacements), les données personnelles étant contenues dans une carte nominative, document papier présenté lors des contrôles. La carte peut être obtenue auprès de commerçants agréés.

2) A l'heure du développement de supports multi-applicatifs (téléphones mobiles NFC entre autres) d'autres cas de figure qu'une carte portant un abonnement peuvent être conçus, par exemple :

- *Une carte utilisable par plusieurs personnes* : cette carte serait souscrite par une personne qui garantirait, par contrat, le paiement des prestations qu'elle contient. La carte anonyme pourrait être utilisée par un groupe de personnes, simultanément (le titulaire, dans ce cas, utilise sa carte, pour payer le voyage de chacun des membres du groupe. Il serait alors nécessaire que la carte puisse être présentée plusieurs fois devant le valideur, donc que la fonction "antipassback" soit désactivée lorsqu'elle est présentée) ou successivement (une mère de famille confie sa carte à ses enfants).

- *Une carte «voyagistes » :* elle pourrait être remise par une agence de voyages à un de ses clients avec des titres chargés correspondants aux déplacements prévus. L'agence serait titulaire de la carte ; le client verserait une caution pour garantir la perte ou le non retour de la carte. Comme dans le cas précédent, cette carte serait anonyme et prépayée et il n'y aurait pas de restriction quant à son utilisation.

3) L'exemple du télépéage

Des explications ont été demandées sur les motifs qui peuvent justifier, au regard du droit des données personnelles, la différence de traitement du système de télépéage « LIBERT'E » par rapport à la télé- billettique.

Lé télépéage autoroutier correspond à un abonnement souscrit par un particulier ou une entreprise pour lui permettre de disposer d'un badge reconnu aux barrières de péage. N'importe quel conducteur d'un même véhicule peut l'utiliser ; il peut être utilisé dans plusieurs véhicules de la même catégorie.

On se trouve dans une situation comparable aux situations qui viennent d'être exposées. Ile télépéage ne pose donc pas les problèmes de traçabilité des déplacements que pose la carte billettique nominative affectée à une personne identifiée qui peut seule l'utiliser. Seul le formulaire rempli au moment de la souscription du contrat contient des données nominatives et est soumis aux restrictions communes à tous les fichiers (droit d'information, droit de rectification).

4) La question tarifaire

Si on étend un peu plus loin le raisonnement consistant à lier le déplacement à l'intérieur d'une agglomération à une activité touristique, on peut imaginer un supermarché proposant d'offrir gratuitement ou à prix préférentiel à ses clients le coût de leurs déplacements pour qu'ils se rendent à son enseigne, celui-ci réglant le prix normal de la course au transporteur. Dans ce cas, la carté délivrée devrait également ne pas concerner qu'une seule personne disposant de droits qui lui sont attachés.

La banque ACCORD, filiale du groupe AUCHAN se penche sur ce type de formule. La question posée est celle de la tarification de la course qui pourrait être meilleur marché que le prix défini par l'autorité organisatrice.