Le passe Navigo anonyme revisité

Pr Michel Arnaud

MoDyCo
Université Paris Ouest Nanterre la Défense CNRS
UFR LL Phi bâtiment L 214
200 avenue de la République
92001 Nanterre Cedex
Michel.arnaud@u-paris10.fr
Tél : 06 85 73 40 57

Résumé

Le passe Navigo anonyme pourrait parfaitement fonctionner gratuitement s'il n'y avait pas un blocage entre la CNIL et la RATP : la CNIL demande l'anonymisation des données de transit quasi immédiatement tandis que la RATP soutenue par le STIF voudrait pouvoir les exploiter davantage. L'exemple de la carte électronique de transport hollandaise (OV chipcard de Translink) et allemande (chipcard de la VDV) montre la combinaison possible d'une carte anonyme avec des données de transit personnalisées. La raison des divergences observées provient du fait que la notion de données personnelles est abordée de manière différente en France et dans d'autres pays européens tels que la Hollande et l'Allemagne. La définition du rôle et des responsabilités du tiers de confiance permettrait de mieux contrôler le lien entre données personnelles et données de transit avec l'arrivée des titres de transport dématérialisés.

Mots clés

Passe Navigo découverte, données personnelles, anonymat, tiers de confiance

Summary

Navigo pass could be offered for free if there was no opposition between CNIL and RATP : CNIL asks for immediate anonymisation of transit data while RATP supported by STIF would like to make use of them. The example of the Dutch OV chipcard of Translink and of the German VDV chipcard shows a possible combination of anonymous card with personalised transit data. The reason for observed divergences comes from the notion of personal data which is handled differently in France and other European countries such as the Netherlands and Germany. Definition and role of trusted third party would allow to better control the link between personal and transit data with the coming of age of electronic ticketing

Key words

Navigo pass discovery, personal data, anonymity, trusted third party.

1. Introduction

Le passe Navigo est une carte à puce sans contact, utilisant la technologie RFID, associant deux technologies : la carte à microprocesseur et la transmission radio des données par radio-identification. Il sert de support pour des forfaits d'abonnement utilisables dans les transports en Île-de-France sur les réseaux RATP, SNCF et Optile. Sa mise en œuvre à partir de 2001 a été supervisée par le STIF, qui est propriétaire de la marque. Cette avancée technique a permis aux transporteurs concernés en Ile-de-France aussi bien que dans d'autres zones en France et ailleurs dans le monde de se débarrasser des péages magnétiques devenus une source de coûts récurrents.

Si la liberté de circulation peut être entravée par la traçabilité permise par le passe électronique, des mesures ont été prises pour la limiter le plus possible en contrôlant la durée de rétention des données et en les anonymisant le plus vite possible. Au-delà de ces mesures ponctuelles plus ou moins bien implémentées du fait des limites de l'action de la CNIL, la question du tiers de confiance se pose avec la dématérialisation du titre de transport sur téléphone mobile. La gestion du lien entre données personnelles et données de transit pourrait lui être confiée. C'est ce qui ressort de l'analyse du cas de la RATP avec le passe Navigo et de celui des partenaires de transport européens.

2. La liberté de circulation entravée par la traçabilité du passe électronique

2.1. L'avènement du passe Navigo depuis 2001 a changé la donne dans les transports publics

Les premiers usagers à avoir bénéficié du passe Navigo sont les porteurs de cartes Intégrale à partir de 2001, suivis par les étudiants disposant de la carte Imagine'R en 2002. En février 2005, les Parisiens et les habitants de proche banlieue, zones 1 et 2, abonnés à la Carte Orange se voient proposer le passe sans contact Navigo. En mai 2006, les Franciliens, quelles que soient leurs zones, peuvent disposer de leur abonnement Carte Orange sur passe Navigo. En juillet 2007, le passe Navigo devient compatible avec le système de location de vélo de la ville de Paris, Vélib' Au printemps 2008, les utilisateurs de Carte Orange sont incités à demander un passe Navigo. En octobre 2008, le STIF revendique un taux de 75 % d'utilisation de Navigo et annonce la suppression de la Carte Orange pour février 2009.

Du côté du voyageur utilisant le passe Navigo et qui peut passer le portillon sans contact en l'effleurant simplement, on peut parler d'une simplification de la procédure. La radiotransmission des informations sur l'abonnement de l'usager aux bornes de contrôle permet de gagner du temps et d'augmenter la fluidité de passage aux valideurs contrôlant les portillons.

Du côté du transporteur et de l'autorité de transport, l'usage d'une carte à puce RFID comme c'est le cas avec le passe Navigo permet d'enregistrer les passages au valideur d'un passe identifiable par son numéro de série. Les types de données collectées par le valideur connecté au fichier des données de validation concernent les informations relatives aux trajets

des usagers, correspondent au moment et au lieu où le voyageur a validé son passage au portillon électronique contrôlé par le valideur Navigo en plus du numéro de passe et du type de contrat et de sa validité. Ces données de validation sont utilisées pour deux usages : la détection de la fraude technologique et la gestion des statistiques de trafic. La procédure de validation du passe Navigo est obligatoire à l'entrée de chaque transport car elle permet de connaître la fréquentation d'une ligne ou d'un arrêt associé à un horodatage et de vérifier que l'abonnement est payé, mettant en évidence les cartes volées et de les rendre invalides sur le réseau.

Les fichiers clients par ailleurs sont constitués au moment de la souscription du passe Navigo et comportent les données personnelles des voyageurs. Le lien entre le fichier des données de validation et celui des données personnelles est réalisé par le numéro du passe. Le fait que les mouvements des voyageurs usagers des transports en commun soient enregistrés a été considéré comme une atteinte à la vie privée et aux libertés individuelles par la société civile et par la CNIL. Le numéro du passe permet en effet de faire le lien entre les données personnelles des usagers et les données de validation, mettant en place les conditions d'une traçabilité constante des déplacements de tel ou tel voyageurs usager du réseau francilien avec un passe Navigo.

2.2. La réaction de la société civile et de la CNIL

La liberté d'aller et venir est un droit fondamental, reconnu dans la Déclaration universelle des droits de l'homme. Elle est inscrite dans la Convention de sauvegarde des droits de l'homme du Conseil de l'Europe tout comme dans le traité de l'Union Européenne. En France, c'est un droit constitutionnel. La société civile s'est mobilisée contre le passe Navigo : l'association des Big Brother Awards a nominé 5 fois le passe Navigo, les collectifs « Souriez vous êtes filmés! » et le Réseau pour l'abolition des transports payants (RATP) l'ont stigmatisé.

Au cours d'une enquête menée en 2002, la Commission nationale de l'informatique et des libertés (Cnil) a étudié les cartes sans contact délivrées dans les transports collectifs comme le passe Navigo et constaté que les déplacements des personnes utilisant ces cartes pouvaient être reconstitués et n'étant plus anonymes, le traitement de ces information était de nature à porter atteinte tant à la liberté d'aller et venir qu'au droit à la vie privée. La CNIL a décidé d'émettre une recommandation afin que la collecte et le traitement d'informations nominatives par les sociétés de transports collectifs dans le cadre des applications billettiques soient conformes aux principes de la loi informatique et libertés du 6 janvier 1978.

Cette recommandation adoptée le 16 septembre 2002 relève en préambule que «les traitements automatisés mis en oeuvre pour assurer le bon fonctionnement de ces titres billettiques créent un risque sérieux en matière de protection des données personnelles. En effet, 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».

2.2.1. Limitation à deux jours du lien entre données personnelles et de validation

La CNIL a préconisé notamment que les données relatives aux déplacements des personnes ne soient utilisées sous une forme permettant d'identifier les usagers que dans le cadre de la lutte contre la fraude et que pendant le temps nécessaire à la détection de la fraude, ce délai ne devant pas excéder deux jours consécutifs. «Les données relatives aux déplacements des personnes, sous la forme d'une indication de la date, de l'heure et du lieu, associées à un élément permettant d'identifier la personne à laquelle elles sont rattachées, tels un numéro de carte, ne devraient être conservées que le temps nécessaire à la détection de la fraude. Ce délai ne devrait pas excéder deux jours consécutifs, y compris le délai de sauvegarde.» Dans le cas d'une fraude avérée, ces données ne devraient être conservées que «le temps de l'instruction de l'affaire par les autorités judiciaires».

Les transporteurs doivent se conformer à ces préconisations. Pour le système de gestion de la fraude, le numéro du passe est indispensable notamment pour s'assurer que celui-ci a bien été émis par un transporteur et que le contrat qu'il contient a bien été vendu. A la RATP, les fichiers de validation sont détruits dès la fin de leur traitement, généralement au bout de quelques dizaines de minutes. Le délai de 48 heures est un délai maximum imposé à tous les responsables de traitement informatique.

Enfin, pour la Cnil, la lutte contre la fraude ne justifie pas le fichage systématique des trajets effectués par les usagers. Le nombre de validations du titre de transport enregistrées sur la carte, «qui varie actuellement entre 2 et 6, devrait à l'occasion du passage à la prochaine génération de cartes, être limité à quatre». De même, la Commission a souhaité que soit offerte à l'usager la possibilité de refuser la «conservation, sous une forme numérique» de la photographie devant figurer sur le titre de transport.

En réponse à cette recommandation, la RATP, a décidé de garder les trois dernières validations dans le passe du voyageur pour permettre le contrôle des titres de transport sur les réseaux. Elles permettent à un contrôleur de vérifier que le trajet effectué correspond bien à l'abonnement contenu dans la carte. La limitation à trois validations permet d'avoir dans la majorité des cas l'ensemble des correspondances effectuées par un voyageur pour un trajet « aller simple ».

Pour le système qui permet d'avoir des données de trafic, la connaissance du numéro du passe est inutile. Ce numéro est modifié par un algorithme qui ne permet pas de revenir au numéro initial. C'est à partir de ces données que sont établies les statistiques de trafic et d'usages des différents moyens de transport.

2.2.2. Préservation du droit à voyager de manière anonyme

Concernant la nature des informations collectées, la Cnil a émis plusieurs recommandations visant à encadrer les pratiques en vigueur. « Les traitements appliqués aux données relatives aux déplacements des personnes devraient être anonymisés, à l'exception de ce qui relève de la gestion de la lutte contre la fraude. En toute hypothèse, il est hautement souhaitable que la possibilité de circuler de façon anonyme, au moyen d'un titre billettique ou non, soit maintenue».

Dans son avis du 8 avril 2004 relative à l'exploitation des données de validation des passes Navigo par la RATP, la CNIL avait estimé « qu'il convenait de laisser aux usagers la

possibilité d'utiliser un service de transport public de manière anonyme, sans qu'il en résulte un surcoût par rapport au choix d'un passe nominatif ». En effet, les données de validation (dates, heure et lieu de passage) sont associées dans le passe Navigo aux numéros d'abonné durant 48 heures, uniquement à des fins de lutte contre la fraude.

Le Syndicat des Transports d'Ile-de-France (STIF) avait alors indiqué qu'une nouvelle forme de passe Navigo, pour lequel les données de validation ne seraient pas associées à un numéro d'abonné (ce qui le rend anonyme), serait mis en vente dès le 1er septembre 2007. Ce nouveau passe se compose d'une carte à puce anonyme et d'une carte nominative de transport qui, pour les besoins des contrôles par les sociétés de transport, comporte au recto les données personnelles suivantes :

- une photographie (collée par l'usager)
- les nom et prénom de l'usager (via une inscription manuscrite).

La carte nominative de transport et la carte à puce doivent être présentées ensemble lors d'éventuels contrôles. En cas de perte, de vol, de détérioration ou d'erreur technique, le remplacement du passe s'effectue moyennant finance à charge pour l'abonné de fournir une nouvelle photographie et de réinscrire ses nom et prénom au recto du nouveau passe.

La carte anonyme, dite passe Navigo découverte, comme le passe Navigo classique, enregistre les déplacements (lieu, date et heure) des usagers mais n'identifie pas l'utilisateur. Les données de validation inscrites sur la puce n'étant pas associées à un numéro d'abonné ou à un nom de client, elle ne sont conservées qu'à des fins purement statistiques et de lutte contre la fraude technologique.

La CNIL s'est réjouie de cette annonce mais a ajouté qu'elle regrettait « la mise en service tardive et payante de ce passe Navigo anonyme », la fourniture de ce support spécifique étant en effet facturée 5 €. Pour contrebalancer ce coût, il a une durée de vie annoncée de dix ans. Les statistiques d'adoption par les usagers montrent qu'au 31 janvier 2009 sur un total de 4 536 000 passes Navigo en circulation, 4 147 00 sont des passes personnalisés (classique, Intégrale, Imagine'R) et 389 000 des passes Découverte anonymes.

Le 6 janvier 2009, après des plaintes de consommateurs et des opérations de « testing » sur le terrain, la CNIL a estimé que l'exercice du droit des usagers à se déplacer anonymement n'était pas garanti car les conditions d'information et d'obtention du passe Navigo découverte étaient particulièrement médiocres, voire dissuasives (manque de sensibilisation du personnel concernant la vente de ce passe, absence régulière de documentation commerciale et difficultés pratiques à l'obtenir au guichet). Fin 2009, la CNIL a pu constater que le passe Navigo était offert dans tous les points de vente de la RATP mais a redemandé au STIF d'aligner les conditions de vente du passe Navigo découverte (anonyme) sur le passe personnalisé. L'argumentaire pour justifier le prix de 5 euros du passe Navigo anonyme du côté des transporteurs est de déclarer qu'il doit y avoir une sanction à sa perte : il s'agit de responsabiliser financièrement le client sur la conservation du support dont la durée de vie est de 10 ans.

Par ailleurs, s'agissant toujours de la diffusion du passe Navigo découverte, la CNIL, été saisie de plusieurs plaintes de la part d'usagers bénéficiant de la tarification solidarité transport applicable aux titulaires du RMI ou de l'allocation spécifique de solidarité. Ces derniers protestaient contre la décision du STIF de leur imposer de souscrire au seul passe

nominatif Navigo et en excluant le passe Navigo découverte anonyme, pour bénéficier de la tarification spéciale.

L'argumentaire des transporteurs et de l'autorité de transport pour justifier le non usage du passe anonyme pour la gestion des clients bénéficiant da la carte solidarité Transport – forfaits gratuité ou tarif réduit 75% est qu'il est nécessaire de disposer dans un fichier client des informations précisant ce droit dont la validation s'exerce sous le contrôle des Présidents de Conseil Général.

La CNIL considère pourtant que rien ne justifie, sur le plan technique, une telle exigence. Aussi, afin que le droit d'aller et venir anonymement soit garanti pour tous, y compris les personnes les plus modestes, titulaires du RMI, la CNIL demande au STIF et à la RATP de permettre, sans délai, aux bénéficiaires de la tarification solidarité transport de pouvoir, s'ils le souhaitent, utiliser le passe Navigo découverte, sans perdre les avantages qui leur ont été reconnus.

2.3. D'autres passes que le Navigo posent plus de problèmes de libertés publiques

Le passe Navigo bénéficie d'une couverture médiatique sans faille car il est utilisé à Paris. Les transporteurs sont soumis à un contrôle quasi permanent de la CNIL. Mais d'autres passes de transport utilisant la RFID sont en fonction en France et ne respectent pas les injonctions de la CNIL. Alex Turk reconnaissait lui-même aux 5èmes assises du correspondant informatique et libertés le 5 juin 2009 que la CNIL ne couvre que moins de la moitié du territoire français, qu'elle n'intervient que dans les grandes villes et que la fonction de correspondant informatique et libertés s'est développée dans les grandes entreprises privées alors qu'il aurait voulu qu'elle le soit aussi dans les collectivités territoriales. Prenons l'exemple de la carte Optymo du Syndicat Mixte des Transports en Commun du territoire de Belfort (SMTC). Ce passe fonctionne sur le principe de la post-facturation. Le SMTC ne vend plus de titres à bord de ses véhicules depuis 2008. La carte Optymo, mise en service en janvier 2008, est gratuite et est associée à un système de post-facturation et de paiement par prélèvement. Les usagers d'un certain âge habitués à payer avec des tickets papier ne peuvent plus le faire. Ils sont même dissuadés de payer en liquide au guichet pour leur passe électronique car les prélèvements sont préférés. Il n'y a pas de carte Optymo anonyme pas plus que de correspondant informatique et libertés à la SMTC.

Dans ce contexte, on peut comprendre pourquoi la police a voulu accéder aux données de Navigo en juin 2008. Selon les informations du Parisien du 21 juin 2008, des policiers de la deuxième division de police judiciaire ont en effet demandé à la RATP de lui fournir les données du passe Navigo du suspect d'une agression commise dans le métro parisien, afin de retracer ses déplacements et de retrouver sa trace. La régie a opposé une première fin de non recevoir à la requête des enquêteurs au motif que celle-ci serait contraire à la protection de la vie privée. La RATP a rejeté peu de temps après une deuxième demande des policiers, en affirmant que les données en questions n'étaient "pas disponibles". Cette affaire est intervenue alors que de nombreux usagers ont fait part de leurs craintes quant aux dangers que fait peser le passe Navigo sur la protection de la vie privée. Le syndicat Alliance Police nationale a de son côté réagi en demandant une "position claire sur l'exploitation des données informatisées". "Comment expliquer qu'une police moderne ne puisse obtenir de telles informations? Il y va de la protection de nos concitoyens", a affirmé le syndicat. Interrogée par un journaliste du Parisien, la RATP a réaffirmé son opposition à une utilisation policière de ses données : "Nous garantissons l'anonymat des déplacements",

affirme la régie. « Les seuls éléments que nous puissions transmettre sur réquisitions judiciaire, sont les trois dernières validations effectuées. Nous restons scrupuleusement dans les termes que la loi nous impose, conformément à la délibération de la Cnil. ». Dans d'autres systèmes de télébilletique, les garde-fous ne sont pas respectés.

La CNIL a prononcé le 20 janvier 2009 un avertissement à l'encontre de la société des transports urbains rennais, considérant que le passe Korrigo ne respectait pas la vie privée et les libertés individuelles des usagers. Saisie de plusieurs plaintes concernant le passe de transport Korrigo anonyme (pour lequel ni le nom ni l'adresse ne sont enregistrés), en raison d'une information jugée quasi-inexistante et de tarifs supérieurs à celui du passe nominatif, la CNIL a diligenté un contrôle dans les locaux de la société Kéolis Rennes. Ce contrôle a souligné de véritables obstacles pour souscrire un passe anonyme. Celui-ci est effectivement plus coûteux que le passe nominatif, seuls des tickets à l'unité pouvant y être chargés et non un abonnement. Le passe anonyme coûte ainsi entre 2,5 et 4 fois plus cher que le passe nominatif, selon l'âge de l'utilisateur. En outre, la très faible information diffusée par la société sur son existence ne permet pas une promotion égale des deux types de cartes. Seuls 53 passes anonymes ont d'ailleurs été distribués contre 186 650 passes nominatifs. La formation de sanction de la CNIL a donc estimé que le respect de la vie privée et de la liberté d'aller et venir anonymement impliquait que les voyageurs disposent d'un véritable choix entre des déplacements anonymes ou nominatifs, ce qui suppose que ceux-ci soient réalisés dans des conditions équivalentes.

D'autres manquements à la loi Informatique et Libertés ont également été relevés. Ainsi la CNIL a constaté que les données personnelles des clients détenant un passe Korrigo étaient conservées sans limite et qu'ils n'étaient pas informés de leurs droits (droit d'accéder à leurs données, de les faire rectifier ou supprimer). Enfin, si la société a pris des mesures pour renforcer la sécurité de l'accès à ses postes informatiques, aucune politique globale de sécurité et de confidentialité des données n'a réellement été formalisée.

3. L'émergence du tiers de confiance

La RATP a testé avec tous les opérateurs téléphoniques l'utilisation du téléphone mobile NFC comme passe Navigo. Basée sur la même technologie, elle a pour objectif de tester l'utilisation du téléphone dans l'usage quotidien du transport. Le passe fonctionne même dans le cas où le téléphone est éteint ou sans batterie. À terme, l'usage des téléphones mobiles comme support des passes devrait permettre de remplacer les tickets à l'unité, voués à disparaître. Ce support télébillétique devrait permettre aussi à terme de charger un type de billets dématérialisés en complément d'abonnement et pourrait même servir de porte-monnaie électronique ou pour gérer le stationnement.

Le rapport d'études (mai 2009) de la Caisse des Dépôts « Le numérique pour plus de mobilité dans les territoires. Panorama et perspectives » fait observer que « l'introduction d'un support dématérialisé impose toujours une évolution de l'écosystème et du modèle économique, ne serait-ce que par l'implication de nouveaux acteurs (technologiques) et par la nécessité de mettre en place une entité de compensation, chargée de gérer la répartition des revenus issus des transactions entre les acteurs. » Pourtant « un consensus sur les dates de cette généralisation, sur un modèle économique, sur le rôle des différents intervenants et sur l'organisation par rapport à la billettique existante n'arrive toujours pas à se dégager. La lenteur des structures de pilotage semble rester un handicap pour le déploiement à moyen

terme de la télébillettique NFC, alors que l'opportunité d'ancrer le standard français sur des standards internationaux devient une nécessité. »

Élément clé du dispositif, comme l'explique l'étude, le choix du gestionnaire du *secure element* est l'une des décisions importantes à prendre pour clarifier l'écosystème et procéder à une première sécurisation du système. Ce gestionnaire a en charge la gestion de l'élément de sécurité du dispositif qui, une fois intégré dans un mobile, va héberger les différentes applications, permettre leur fonctionnement de manière indépendante et gérer des fonctions de contrôle et d'authentification. En France, les opérateurs télécoms pourraient remplir ce rôle si l'on suit les principes de l'architecture SIM centric, dans laquelle les applications sans contact sont hébergées sur la carte SIM du téléphone.

La confiance entre les opérateurs mobiles et les fournisseurs de services est elle aussi un facteur décisif pour développer la dématérialisation des titres de transport via le mobile NFC. En effet, les fournisseurs de services, souvent concurrents, ont besoin de garanties en termes de sécurité, de confidentialité et de qualité de service. La solution évoquée serait l'émergence d'un acteur tiers, ou tiers de confiance (TSM : Trusted Service Manager) pour structurer le marché, réguler, arbitrer certaines positions et envoyer des signes de confiance aux acteurs. Il aurait en charge la gestion des téléchargements de données vers la carte SIM et des applications pour le prestataire de services (opérateur de transport, par exemple), la gestion des accès aux données sensibles. Au-delà du rôle technique, il aurait un rôle d'intermédiaire de confiance dans la relation économique et juridique sur l'ensemble de la chaîne.

3.1. Le fichier clients à protéger par le tiers de confiance

Le contexte des processus Navigo Multi-Contrats (NMC) repose sur deux systèmes qui communiquent entre eux : le SIG : Système d'Information et de Gestion, qui gère les clients, les contrats et les passes, détenu par le GIE COMUTITRES et les ***SYDEF*** : Système de détection de la fraude, qui existent chez chaque transporteur : RATP , SNCF et OPTILE. Le SYDEF ne connaît pas le nom des clients mais seulement des numéros de passes. Le transporteur ne voit circuler sur son réseau que des numéros de passes. Les deux systèmes ne communiquent que par échange de listes : liste noire et blanche mais ne sont pas connectés pour croiser des informations. Les données nominatives restent pendant 24-48h chez les transporteurs, c'est à dire que l'on est capable de dire que *« le passe 063877733 a validé son abonnement à la gare St Lazare au tourniquet n°234 à 8h45 »*, puis ces données sont dites statistiques parce qu'elles ont été anonymisées entre temps. C'est-à-dire qu'on n'est plus capable d'identifier le propriétaire du passe. Un passe anonyme ne permet pas de se connecter au fichier clients puisqu'il n'y a pas d'identification de l'acheteur de ce passe dans le SIG. Il n'y a pas de lien possible entre le fichier clients SIG et le fichier de validation SYDEF (correspondant aux passages aux tourniquets).

Dans le cas du passe Navigo gratuit nominatif, les informations relatives au client sont stockées dans le SIG. A partir du lien entre les infos client et le numéro du passe, ce dernier est fabriqué. Le poste agence est connecté en permanence au SIG qui pilote la caméra pour prendre la photo et imprimer le passe. Les transporteurs ont défini une liste blanche pour contrôler les passes qui circulent sur le réseau et pour détecter les cartes falsifiées. Cette liste est gérée par le SIG où se retrouve a minima le numéro du passe. L'association du numéro de carte (passe) et de contrat, permettant de vérifier la vente, constitue l'acte de validation. C'est ce lien qui est détruit dans les 48 heures sur les injonctions de la CNIL (avec un hash code)

pour garder seulement les données liées au déplacement pour les exploitations statistiques. Ces données sont détruites dans le SYDEF mais pas dans le SIG.

L'architecture du SIG parce que découplé du SYDEF donne toutes les facilités à un organisme qui pourrait jouer le rôle du tiers de confiance, que ce soit la RATP, la SNCF, COMUTITRES, le STIF. Le SIG répond tout a fait à ces attentes, car il décorrèle complètement la partie gestion des passes et l'utilisation sur les réseaux. Le cabinet d'avocat Alain BENSOUSSAN a rédigé la déclaration CNIL du SIG et a constaté ces possibilités.

Le tiers de confiance pourrait générer un pseudo certifié garantissant:
- que le contrat de vente a bien été passé,
- que la carte (passe) est valide,
- l'anonymat du voyageur.

Est-ce que la CNIL serait d'accord ? L'exemple du dossier médical personnel tend à le démontrer puisque la CNIL a émis en 2006 l'avis suivant : « Un numéro identifiant santé spécifique, dénommé NIS, identifiera le patient concerné et garantira contre les doublons et les risques de collisions. Son processus de création par le GIP-DMP (Groupement d'Intérêt Public Dossier Médical Personnel) fera intervenir un tiers de confiance, la Caisse des dépôts et consignations, membre du Conseil d'administration du GIP-DMP. Ce numéro sera, comme la CNIL l'avait souhaité, déconnecté du numéro de sécurité sociale.»

3.1.1. Les données anonymes personnalisées

Seulement le numéro de contrat, le numéro de carte, le lieu et la date (3 voyages au maximum) sont numérisés sur le passe Navigo (carte calypso) et par conséquent lus par le lecteur de carte au moment de la validation correspondant au passage du voyageur. La gestion de la carte solidarité transport, forfait gratuité ou tarifs réduits à 75% s'appuie sur un fichier clients géré par le Conseil Général du département concerné qui garantit l'existence de droits correspondants pour les personnes pouvant en bénéficier. Dans ce cas, le Conseil Général agirait comme tiers de confiance puisqu'il garantit que la personne identifiée a bien droit aux facilités allouées. Ce fichier du Conseil Général est fourni chaque année à Comutitres et donne l'accès à une carte CST au titulaire, tout étant géré dans le SIG.

Dans ce contexte, le passe Navigo découverte devrait certifier le statut du titulaire de la carte sans pour autant révéler son identité. Le principe de la carte d'identité blanche de Deswartes est intéressant à cet égard : il s'agit d'associer un marqueur sur l'identité du porteur de la carte dans la carte elle-même sans révéler ses données personnelles. Certifier son identité est possible par une reconnaissance biométrique par exemple : le porteur de la carte est identifié parce que le lien avec sa carte est authentifié. Pour gérer cette option, il faudrait ajouter des éléments de biométrie sur le passe Navigo. Ce qui se passe en Belgique est révélateur de la tendance : il est possible depuis fin 2009 d'acheter son titre de transport SNCB sur Internet et de le charger sur sa carte d'identité électronique. Dans ce cas, tout est révélé : l'identité du porteur de la carte, ses données personnelles, son titre de transport. Dans le cas qui nous occupe, il serait possible de faire certifier le lien entre les données biométriques sur la carte et le porteur de la carte par le tiers de confiance sans pour autant révéler les données personnelles du voyageur au contrôleur. La notion de pseudo certifié correspond à cette approche.

En conclusion provisoire, il y a plusieurs statuts d'anonymat plus ou moins renforcés tout comme des niveaux de personnalisation. Il convient d'étudier les dispositifs utilisés par

les transporteurs et négociés avec les utilisateurs dans les Etats membres de l'Union européenne pour être informés des options choisies et en tirer les leçons en termes de bonnes pratiques relatives à la protection des données personnelles des voyageurs.

3.2. Le lien avec les données personnelles à confier au tiers de confiance

En Hollande, la carte OV-chipcard du système de transport national Translink est proposée avec quatre options :

- complètement anonyme (aucune information personnelle sur la carte),
- anonyme avec un porte-monnaie électronique permettant de se connecter à un compte bancaire (zones étanches sur la carte faisant qu'elle est partiellement personnalisée),
- anonyme personnalisé (correspondant à l' « opt in ») : certaines données personnelles sont communiquées avec l'accord du propriétaire de la carte aux partenaires commerciaux du transporteur sans révéler l'identité du voyageur sur la carte (aucune donnée personnelle disponible sur la carte),
- personnalisée (nom, date de naissance, photo imprimés sur la carte, le numéro de la carte et les dix dernières transactions numérisés dans la carte).

En Allemagne, la carte chipcard est proposée par le consortium VDV avec les mêmes quatre options. Ces facilités correspondent à des variations dans l'application de la définition des données personnelles telle qu'elle figure dans la directive européenne 95-46. Chaque Etat membre a une manière d'interpréter la directive dans le cadre de la subsidiarité en fonction des pratiques en vigueur sur son territoire. Le G29 ne peut que se faire l'écho de ces divergences. L'aspect indirect du lien entre données personnelles et données de transit (validation) est apprécié différemment selon les pays. La France a une approche stricte : tout lien même indirect avec les données personnelles est susceptible d'être activé et de générer une violation de la vie privée du voyageur. En Hollande, la difficulté de faire ce lien est appréciée : si le lien demande un excès de développement pour être activé, les données de transit ne sont pas considérées comme données personnelles. Ainsi le concept d'anonymat personnalisé peut se faire jour : on peut dévoiler les habitudes de transport d'un voyageur sans pour autant révéler son identité. Dans ce type de configuration, le rôle du tiers de confiance devient central car il est chargé d'assurer la protection de l'identité du voyageur tout en permettant différents arrangements en fonction des choix de ce dernier, en particulier dans le cadre de l'option où il décide de révéler certaines données de transit (« opt in »).

4. Conclusion

L'arrivée des titres de transport sur téléphones mobiles pourrait être l'occasion d'une remise à plat de la loi informatique et libertés. La directive européenne 95-46 va être révisée par la Commission européenne. Il n'est certainement pas question de remettre en cause les principes de la protection des données personnelles mais plutôt de revoir leurs modes d'application. Il conviendrait non seulement de renforcer les pouvoirs de la CNIL comme le prévoit le projet de loi du Sénat, mais aussi de revoir l'appréciation du lien entre données personnelles et données de transit. Au lieu de déclarer que tout lien même indirect doit être rompu pour garantir l'anonymat et d'y veiller, il vaudrait mieux moduler cette position en déléguant la gestion de ce lien au tiers de confiance dont le rôle et la responsabilité seraient reconnus aux côtés de ceux du responsable du traitement des données. Cette évolution se

produit dans d'autres pays européens. Il serait regrettable que la France en avance en son temps avec la loi informatique et libertés de 1978 en subisse maintenant le préjudice faute de pouvoir la mettre à jour. Dans un monde en constant changement, l'appareil de protection juridique a un temps de retard, ce qui est normal. Toutefois, dans le cas qui nous occupe, il y a risque que les développements techniques et commerciaux mettent à mal les protections établies en les contournant, créant un climat de suspicion de la part des consommateurs, en l'occurrence des voyageurs, confrontés à des offres commerciales sans garanties en contrepartie. A l'heure où le titre de transport européen va se généraliser, l'anonymat des titres de transport électronique est un vrai enjeu qui nécessite que les juristes se penchent sur l'architecture « privacy by design » et définissent le rôle et les responsabilités du tiers de confiance.

5. Bibliographie

Arnaud M., « Authentification, identification et tiers de confiance», dans *Traçabilité et réseaux*, coordonné par Michel Arnaud et Louise Merzeau, Hermès 53, avril 2009, CNRS Editions, Paris, 263 p., pp.129-136

Code of conduct for processing OV-chipkaart personal data by public transport companies. Adopted on 21 June 2007 by Mobis and deposited with the Court in The Hague on 10 July 2007 under number 50/2007. Amended on 6 February 2009 and adopted by the public transport companies that accept the OV-chipkaart and, at their request, deposited by KNV with the Court in The Hague on 13 February 2009 under number 16/2009. Translated by NS Dutch Railways in cooperation with law firm Kennedy Van der Laan

Télébillettique Ile-de-France Étape2 – Définition des données sur la carte STIF/TBTQ/INSTIDF2 version 2.2

Dossier de spécification Interface avec Personnalisateur IPS-327401-0C.doc COMUTITRES

Le numérique pour plus de mobilité dans les territoires. Panorama et perspectives. Rapport d'études. Mai 2009. Caisse des Dépôts. Disponible sur :<http://www.dent.caissedesdepots.fr/spip.php?rubrique5>.(Consulté le 16/05/2010)

Webographie :

Le passe découverte : un passe navigo enfin anonyme ! 5 août 2007. Disponible sur : < http://www.cnil.fr/la-cnil/actu-cnil/article/article//le-passe-decouverte-un-passe-navigo-enfin-anonyme/>. (Consulté le 16/05/2010)

2ème contrôle des passes anonymes NAVIGO. 4 février 2010. Disponible sur : < http://www.cnil.fr/la-cnil/actu-cnil/article/article//2eme-controle-des-passes-anonymes-navigo/>.(Consulté le 16/05/2010)

Avertissement pour le passe Korrigo de Rennes. 17 juin 2009. Disponible sur: < http://www.cnil.fr/la-cnil/actu-cnil/article/article/91/avertissement-pour-le-passe-korrigo-de-rennes/>.(Consulté le 16/05/2010)

Dupont.T., *La Cnil s'inquiète du fichage dans les transports en commun.* Transfert.net, 7 octobre 2003. Disponible sur :
<http://www.zdnet.fr/actualites/internet/0,39020774,39125887,00.htm>.
(Consulté le 16/05/2010)

Manach J.-M., *Le passe Navigo "anonyme" n'existe pas*. 7 janvier 2009. Disponible sur : <http://bugbrother.blog.lemonde.fr/2009/01/07/le-passe-navigo-%E2%80%9Canonyme%E2%80%9D-nexiste-pas>. (Consulté le 16/05/2010)

Philibert M., *Quand la police voulait faire "parler" le pass Navigo.* 22/07/2008. Disponible sur : <http://www.vsd.fr/contenu-editorial/l-actualite/les-indiscrets/729-quand-la-police-voulait-faire-parler-le-pass-navigo?xtor=RSS-1>. (Consulté le 16/05/2010)