

Date de publication sur legifrance: 14/10/2015

Commission Nationale de l'Informatique et des Libertés

Délibération n°2011-107 du 28 avril 2011

Délibération n° 2011-107 du 28 avril 2011 portant autorisation unique de mise en œuvre de traitements automatisés de données à caractère personnel relatifs à la gestion des applications billettiques par les exploitants et les autorités organisatrices de transport publics

(décision d'autorisation unique n°AU- 015)

La Commission nationale de l'informatique et des libertés,

Vu la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales du 4 novembre 1950.

Vu la convention n°108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

Vu la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement de données à caractère personnel et à la libre circulation de ces données ;

Vu la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée par la loi n°2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, notamment ses articles 1er et 25-II ;

Vu le décret n°2005-1309 du 20 octobre 2005 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifié par le décret n° 2007-451 du 25 mars 2007 ;

Vu l'article 9 du Code civil ;

Vu les articles 226-16 à 226-24 du code pénal ;

Vu la délibération n° 03-083 du 16 septembre 2003 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 billettique ;

Après avoir entendu M. Eric PERES, Commissaire, en son rapport et Mme Elisabeth ROLIN, Commissaire du gouvernement en ses observations.

Formule les observations suivantes :

La modernisation des transports collectifs se traduit notamment par la délivrance de nouveaux titres de transport aux usagers, sous différents supports utilisant une technologie sans contact, en vue de faciliter leurs déplacements et de leur proposer des services complémentaires.

L'interopérabilité des systèmes permet, en outre, de voyager avec le même billet sur plusieurs

réseaux et favorise l'harmonisation de la gestion des titres de transport.

Outre l'utilisation des titres de transport, le dispositif billettique vise à assurer la réalisation d'analyses statistiques, la mesure de la qualité du fonctionnement du système, la détection de la fraude technologique et le suivi des impayés : il y a lieu, à cet effet, de préciser que l'inscription d'une personne en liste d'opposition à la suite d'un impayé a pour effet d'invalidier son passe billettique et ainsi ne lui permet plus d'utiliser ce type de titre de transport jusqu'à la régularisation des sommes dues.

La Commission considère, en conséquence, qu'il y a lieu, dès lors, de faire application de l'article 25-I-4° de la loi du 6 janvier 1978 modifiée en août 2004 qui soumet à autorisation préalable de la CNIL « 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 ».

Cette autorisation peut prendre la forme d'une décision unique en application de l'article 25-II de la loi du 6 janvier 1978 susvisée dès lors que les traitements répondent à une même finalité, portent sur des catégories de données identiques et ont les mêmes destinataires ou catégories de destinataires.

Ainsi l'organisme de transport collectif qui envisage de mettre en œuvre un traitement de données à caractère personnel ayant pour finalité la gestion des applications billettiques, pourra, s'il respecte les dispositions de la décision unique, adresser à la Commission un engagement de conformité aux caractéristiques de l'autorisation.

L'utilisation d'un titre de transport sans contact implique la collecte de données concernant les trajets effectués par le titulaire lors de la validation, c'est-à-dire de la présentation du titre de transport à une borne de contrôle en entrée et sortie du réseau ou à l'occasion d'une correspondance. Peuvent ainsi être mémorisés, tant sur la carte qu'au poste central de l'exploitant de transport, non seulement les date, heure et lieu des passages mais aussi le numéro de carte utilisé qui rend possible, à partir du fichier clientèle, l'identification du titulaire de la carte. Dès lors, les déplacements de ce dernier peuvent être reconstitués et ne sont plus anonymes, ce qui est de nature à porter atteinte tant à la liberté fondamentale d'aller et venir, qu'au droit à la vie privée. Le respect de ces principes justifie ainsi une vigilance particulière de la CNIL lorsqu'elle doit apprécier la pertinence des données collectées, conformément à l'article 6 de la loi Informatique et Libertés.

La possibilité de circuler de façon anonyme doit, dans tous les cas, être préservée : chaque responsable de traitement qui met à disposition des usagers des titres nominatifs de transport doit également prévoir de leur laisser le choix d'utiliser des titres de transport anonymes.

L'autorité organisatrice de transport doit mettre en œuvre, dans la mesure du possible, les moyens nécessaires pour la préservation d'une alternative au titre nominatif quel que soit le type d'abonnements. Elle doit ainsi prévoir des abonnements sur des titres qui préservent l'anonymat des déplacements.

Il existe trois sortes de titres de transport : le titre de transport nominatif (support nominatif, l'utilisateur figure dans le fichier client du transporteur, ses déplacements ne sont donc pas anonymes), le titre de transport déclaratif (le support est nominatif mais l'utilisateur ne figure pas dans le fichier client, ce qui permet un anonymat des déplacements) et le titre de transport anonyme (le support est anonyme, aucun abonnement ne peut donc être chargé dessus).

La Commission s'attache à l'anonymat des déplacements et à la possibilité pour l'utilisateur de ne pas

figurer dans le fichier clients du transporteur et non pas à l'anonymat du support sur lequel est chargé le titre de transport.

Par ailleurs, dans la mesure du possible, les tarifs spéciaux doivent également être disponibles sur titres de transport déclaratifs.

Décide que les responsables de traitement qui adressent à la Commission une déclaration comportant un engagement de conformité pour les traitements de données à caractère personnel répondant aux conditions fixées par la présente décision unique sont autorisés à mettre en œuvre ledit traitement.

Article 1er : Finalités et caractéristiques techniques du traitement

Les traitements de billettique mis en œuvre par les exploitants de transport public ainsi que par les autorités organisatrices de transport doivent avoir pour finalités :

La gestion, la délivrance et l'utilisation des titres de transport :

- gestion des abonnements et délivrance des titres de transport plein tarif, à tarif réduit ou même gratuits ;
- gestion des opérations du service après vente et des réclamations clients.

La gestion et le suivi des relations commerciales :

- gestion des offres commerciales (par exemple : envoi d'offres par les partenaires commerciaux) ;
- gestion des programmes de fidélisation.

La gestion de la fraude :

- détection de la contrefaçon et de la fraude technologique ;
- instruction des dossiers de fraude technologique ;
- gestion des cartes invalidées suite à une perte ou un vol ;
- gestion des cartes invalidées suite à la détection d'un usage abusif (par exemple : détection de plusieurs dizaines de passage avec un même passe) ;
- gestion des cartes invalidées suite à un incident de paiement.

La réalisation d'analyses statistiques d'utilisation des réseaux :

- analyses statistiques du trafic ;
- analyses statistiques de la nature des titres de transport délivrés ;
- analyses statistiques de la clientèle ;
- analyses statistiques d'utilisation par type de titres de transport.

La mesure de la qualité du fonctionnement du système :

- analyses des problèmes techniques liés à la carte ;
- analyses des problèmes techniques liés aux valideurs ;
- détection des anomalies fonctionnelles du système d'information.

Article 2 : Données à caractère personnel traitées

- Au titre des traitements relatifs à la gestion, la délivrance et à l'utilisation des titres de transport billettiques, à la réalisation d'analyses statistiques, à la mesure de la qualité du fonctionnement du système et à la détection de la fraude technologique :

- l'identité (civilité, sexe, nom, prénom) ;
- la date et le lieu de naissance ;
- l'adresse postale ;
- les numéros de téléphone (personnel et portable) et l'adresse courriel (facultatifs) ;
- la photographie ;
- l'identité et l'adresse du payeur lorsque le payeur n'est pas l'abonné ;
- le mode de paiement ;
- en cas de paiement de l'abonnement par prélèvement bancaire : le nom de la banque, l'établissement, le guichet, le numéro de compte et la clé de RIB, la signature de l'abonné, un relevé d'identité bancaire ;
- la situation socioprofessionnelle (étudiant-apprenti, actif, scolaire ou autre) ;
- le nom de l'établissement scolaire ou universitaire ;
- la classe fréquentée à titre facultatif ;
- le numéro de client ;
- l'historique client ;
- le type d'abonnement ;
- les données de validation : date, heure, lieu de la validation ; 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. Ces données 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 ; 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.
- les dates de début et de fin de validité de la carte ;
- le numéro de carte ;
- le motif de l'inscription sur un fichier d'exclusion d'après une liste fermée ;
- une copie de la pièce d'identité (uniquement dans l'hypothèse d'une demande d'abonnement à distance par voie postale ou électronique et non pour une demande au guichet) ;
- une copie d'un justificatif de domicile (uniquement dans l'hypothèse d'une demande d'abonnement à distance par voie postale ou électronique et non pour une demande au guichet).

Le journal des validations enregistrées sur la carte n'est pas consultable aux bornes de consultation en libre service.

- Au titre du post paiement (afin d'établir la facturation des trajets et de permettre la gestion des réclamations) :

Seules les données nécessaires au calcul du prix du titre pourront être collectées en plus de la date et de l'heure.

A ce titre, et uniquement si ces informations sont nécessaires au calcul du prix du titre, le responsable de traitement peut collecter des informations telles que le nombre de trajets, la zone ou la distance du voyage.

En tout état de cause, la collecte du lieu (de la station de validation) pour du post-paiement ne saurait être justifiée et serait de nature à contrevenir à la liberté d'aller et venir anonymement.

- Au titre des traitements relatifs à la gestion des titres de transports gratuit ou à tarif réduit, les catégories de données relatives :

- à la scolarité ;
- au handicap ;
- au bénéfice d'une allocation sociale ;
- à l'âge ;
- aux revenus ;
- au statut de famille nombreuse ;
- au statut d'agents exploitants de transport ou des autorités organisatrices et de leurs ayants-droit.

Les justificatifs fournis pour la délivrance des titres de transport peuvent être scannés et conservés sur le système d'information et directement accessibles en ligne uniquement à des fins d'édition du titre de transport et uniquement le temps de la délivrance du titre. Au-delà, les pièces justificatives ne peuvent être conservées que sur un support indépendant, non accessible par les systèmes de production, n'autorisant qu'un accès distinct, ponctuel et motivé auprès d'un service spécifique seul habilité à consulter ce type d'archive et uniquement à des fins de gestion du titre, de l'abonnement ou du contentieux.

- Au titre des traitements relatifs à la gestion des impayés :
- l'identité (nom, prénom) ;
- la date de naissance ;
- l'adresse ;
- le numéro de compte de l'abonné ;
- le montant de l'impayé ;
- la banque ;
- 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 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.

Des zones bloc-notes peuvent être prévues : les mentions inscrites dans ces zones ne doivent porter que sur des actes et des faits objectifs et ne peuvent, en aucun cas, faire apparaître, directement ou indirectement, des données relatives aux infractions commises par les abonnés et des données relatives aux origines raciales, aux opinions politiques, philosophiques ou religieuses, aux appartenances syndicales ou aux mœurs de la personne concernée par ces actes ou ces faits.

Article 3 : Destinataires des informations

Dans la limite de leurs attributions respectives et pour l'exercice des finalités précitées, seuls peuvent être destinataires des données :

- au titre des traitements relatifs à la gestion, la délivrance et à l'utilisation des titres de transport billettiques, la gestion et le suivi des relations commerciales, la réalisation d'analyses statistiques : les personnes habilitées du service commercial, du service marketing, du service après vente, du service financier, du service juridique et les agents des guichets d'accueil et de vente.
- au titre de la mesure de la qualité du fonctionnement du système et la détection de la fraude technologique : les personnes habilitées du service technique, de la cellule surveillance de la fraude ainsi que les agents de guichet pour le seul besoin d'information.
- au titre des traitements relatifs à la gestion des impayés : les personnes habilitées du service en charge de la gestion des impayés et les agents de guichet, ces derniers n'ayant accès qu'à une

indication de la situation d' « impayé » de l'abonné.

Dans le cadre des dispositifs interopérables, les données du client pourront être échangées entre les réseaux urbains. Toutefois, dans le cadre d'une inscription en liste d'opposition, seuls les numéros des cartes des usagers dont le passe a été invalidé à la suite d'une perte, d'un vol, d'un impayé ou d'un défaut, sont transmis aux sociétés de transport dont les systèmes billettiques sont interopérables, à l'exclusion de toute communication d'autres données à caractère personnel.

Article 4 : Durée de conservation

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.

Dans le cadre des traitements mis en œuvre, 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.

Toutefois, les données de validation contenant des informations relatives aux déplacements des personnes, associées au numéro de carte ou de l'abonné, élément renvoyant indirectement à l'identité d'un usager, pourront être conservées pendant 48h au maximum et aux seules fins de lutter contre la fraude technologique.

Pour permettre la gestion des réclamations dans le cadre du post paiement, les informations nécessaires à la facturation (y compris les données de validation, à l'exception du lieu), peuvent être conservées pendant une durée de quatre mois à compter de la date des événements. Dès lors, un tri doit être opéré dès la centralisation des données de validation dans le système, afin que ne soient conservées pendant cette durée que les données des personnes ayant choisi le post-paiement.

Les informations relatives à la gestion des impayés sont immédiatement retirées de la liste d'opposition dès régularisation des sommes dues ; à défaut de régulation, elles seront conservées pendant au maximum deux ans à compter de l'inscription.

Article 5 : Mesures de sécurité

Des mesures techniques et organisationnelles sont mises en œuvre afin de se prémunir contre les risques d'intrusion et de détournement de données sur les systèmes informatiques. Ces mesures doivent en particulier :

- imposer un contrôle d'accès aux systèmes de gestion des données billettiques, avec une gestion rigoureuse des habilitations ;
- limiter l'accès des paramètres de sécurité et des clés cryptographiques utilisées à un nombre minimal d'intervenants désignés et habilités ;
- mettre en place un système de traçabilité des accès aux données ;
- protéger la confidentialité et l'intégrité des échanges lors du transfert de données billettiques sur tout réseau qui n'est pas exclusivement destiné à véhiculer des données billettiques ;
- protéger de manière adaptée le système d'information contre des intrusions par le réseau ;
- faire l'objet d'audits et de mises à jour.

Ces mesures font l'objet de procédures documentées et dont l'application est vérifiable.

Si l'anonymisation utilise un algorithme de 'hachage', celui-ci est irréversible et doit recourir à une clé cryptographique renouvelable selon une périodicité au moins annuelle. Les valeurs anonymisées produites après un renouvellement de clé ne doivent pas pouvoir être liées à celles qui ont été produites avant celui-ci. La valeur de la clé secrète de 'hachage' utilisée ne doit pas être accessible directement ou indirectement à un seul individu.

Les composants ou les clés sont répartis entre plusieurs organismes ou plusieurs personnes habilitées, chacune ne disposant au plus que d'un composant ou clé, afin de garantir l'objectif de sécurité visé.

Dans le cas où le titre de transport serait utilisé comme support d'identification pour des services autres que du transport collectif, il devra également répondre aux exigences suivantes :

- Les modalités d'utilisation du titre doivent garantir une stricte étanchéité entre les services autres que ceux visant à fournir une offre de transport public. Les identifiants tant techniques que fonctionnels utilisés doivent être uniques pour chaque service, et n'être connus que du fournisseur du service, afin de prévenir tout croisement d'informations entre les services, sauf dans les cas de services de transport public qui peuvent partager entre eux un identifiant unique dans le but d'offrir à l'utilisateur une offre intégrée de transport.
- Cette étanchéité doit également garantir l'impossibilité pour un fournisseur de service (y compris l'exploitant et l'autorité organisatrice de transport) d'altérer le fonctionnement du titre pour les autres services.
- Enfin des mesures doivent également être mises en œuvre afin de garantir à l'utilisateur la faculté de désactiver l'accès à un service à partir de son titre de transport. Cette désactivation doit entraîner la rupture du lien entre le titre et le service.

Article 6 : Information des personnes

Le responsable du traitement procède, conformément aux dispositions de l'article 32 de la loi du 6 janvier 1978 modifiée en août 2004, à l'information des personnes notamment en ce qui concerne la finalité du traitement, le caractère obligatoire ou facultatif des réponses et les modalités d'exercice du droit d'accès et de rectification par un affichage dans les points de délivrance des cartes ainsi que sur les formulaires d'abonnement.

La possibilité d'utiliser des titres de transports déclaratifs et/ou anonymes doit être portée à la connaissance des intéressés selon les mêmes modalités que celles prévues pour les titres de transports nominatifs. Pour les titres nominatifs, il leur est également précisé qu'ils peuvent s'opposer à la conservation de leur photographie au format numérique.

Les personnes concernées sont informées des destinataires des données, notamment dans le cadre d'une interopérabilité des systèmes entre les différents réseaux de transports.

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.

Article 7 : Exercice des droits d'accès et de rectification

Les droits d'accès et de rectification définis au chapitre V de la loi du 6 janvier 1978 modifiée s'exercent auprès du ou des services que le responsable de traitement aura désignés.

Article 8 : Formalités particulières

Tout traitement automatisé de données à caractère personnel, ayant pour objet la gestion des applications billettiques et comptant parmi ses finalités la gestion des impayés, qui n'est pas conforme aux dispositions qui précèdent doit faire l'objet d'une demande d'autorisation auprès de la Commission dans les formes prescrites par les articles 25-I-4° et 30 de la loi du 6 janvier 1978 modifiée.

Les traitements ayant pour finalité la gestion des opérations de contrôle des titres de transport dans le cadre des applications billettiques devront, par ailleurs, faire l'objet d'un engagement de conformité à l'autorisation unique n° 12 adoptée par la délibération de la CNIL n° 2007-002 le 11 janvier 2007 relatif aux traitements ayant pour finalité la gestion des infractions à la police des services publics de transports terrestres ou à défaut d'une demande d'autorisation spécifique auprès de la Commission.

Article 9

La délibération n°2008-161 du 3 juin 2008 portant autorisation unique de mise en œuvre de traitements automatisés de données à caractère personnel relatifs à la gestion des applications billettiques par les exploitants et les autorités organisatrices de transport publics est abrogée.

Article 10

La présente délibération sera publiée au Journal officiel de la République française.

Le Président
Alex TÜRK

Nature de la délibération: AUTORISATION UNIQUE