Délibération n°2009-002 du 20 janvier 2009 de la formation restreinte prononçant un avertissement à l'encontre de la société KEOLIS RENNES

La Commission nationale de l'informatique et des libertés, réunie en formation restreinte, sous la présidence de M. Alex TÜRK, président ;

Etant aussi présents M. Guy ROSIER, vice-président délégué, M. François GIQUEL, vice-président, Mlle Anne DEBET, M. Hubert BOUCHET, membres ;

Vu la Convention n° 108 du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

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 ;

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, modifiée par le décret n°2007-451 du 25 mars 2007 ;

Vu la délibération n° 2006-147 du 23 mai 2006 fixant le règlement intérieur de la Commission nationale de l'informatique et des libertés ;

Vu la décision n° 2008-108 C du 9 octobre 2008 du président de la Commission nationale de l'informatique et des libertés de procéder à une mission de contrôle auprès de la société KEOLIS RENNES ;

Vu le courrier de la société KEOLIS RENNES du 15 janvier 2009 ;

Vu le rapport de Mme Isabelle FALQUE-PIERROTIN, commissaire rapporteur, notifié le 19 décembre 2008 à la société KEOLIS RENNES ;

Vu les autres pièces du dossier ;

Après avoir entendu, lors de la réunion du 20 janvier 2009 :

- Mme Isabelle FALQUE-PIERROTIN, commissaire, en son rapport ;
- Mme Pascale COMPAGNIE, commissaire du Gouvernement, en ses observations ;
- M. C. ;
- M. C, .

M. C. ayant pris la parole en dernier.

I. Faits et procédure

A. Faits

La Commission nationale de l'informatique et des libertés (ci-après « CNIL » ou « la Commission ») a été saisie de plaintes signalant un défaut d'information concernant le passe de transport KORRIGO « anonyme » des transports urbains rennais ainsi que du différentiel de tarif existant entre ce passe et un passe KORRIGO nominatif.

Le dispositif de billettique « KORRIGO » par carte RFID est mis en place par la société KEOLIS RENNES (ci-après « la société »), sous l'enseigne commerciale STAR (société des transports de l'agglomération rennaise). Ce délégataire de service public gérant les transports publics rennais de métro et de bus emploie 800 salariés.

Un correspondant informatique et libertés a été désigné, par la société, le 19 mai 2006.

En application de la décision n° 2008-108 C du 9 octobre 2008 du président de la CNIL, une délégation de la Commission a procédé à une mission de vérification sur place, les 21 et 22 octobre 2008, auprès de la société.

La délégation de la CNIL s'est attachée à examiner plusieurs traitements.

1. Le traitement « Gestion des fiches clients » (GFC) contient l'intégralité des données à caractère personnel des clients disposant d'une carte RFID nominative (les données à renseigner de manière obligatoire sont les nom, prénom, adresse postale, date de naissance, de manière facultative, la photographie, l'adresse électronique, les numéros de téléphone fixe et mobile). En outre, y figurent les numéros de client, numéros des cartes détenues par le client avec les éventuelles inscriptions sur la liste noire et un historique client (« journal »), contenant notamment l'historique des anciennes cartes détenues. L'application dispose, également, d'une zone de commentaire libre (dite « *mémo* ») permettant l'inscription de la mention « impayé en cours ».

La création de ces fiches clients s'effectue exclusivement auprès de l'agence commerciale principale. Le personnel de l'agence en charge de la gestion des clients peut accéder à l'ensemble de l'application, seuls les superviseurs ayant la possibilité de supprimer des fiches clients. Le service comptable, situé au siège administratif de KEOLIS peut également accéder à l'application ainsi que le service informatique.

La délégation a constaté qu'aucune politique de durée de conservation n'a été définie pour toutes ces données.

Le traitement GFC contient, en outre, une fonctionnalité dénommée « *cession en prélèvement automatique* », qui gère les modifications liées à ce mode de paiement (nouvelles données bancaires du client, suspension du prélèvement automatique, résiliation du prélèvement automatique). Après une résiliation, les données bancaires sont conservées durant une durée indéterminée, dans une liste créée spécifiquement et appelée « clients en résiliation définitive PA ».

Il contient également une fonction de « Gestion des impayés », assurée par le service recouvrement. Si le traitement GFC a fait l'objet d'une déclaration n° 1140928, auprès de la CNIL, en décembre 2005, cette fonctionnalité n'avait pas été déclarée à la Commission au

jour du contrôle (la société a procédé, le 7 novembre 2008, à un engagement de conformité à l'autorisation unique n° 15 relative à la gestion des applications billettiques par les exploitants et les autorités organisatrices de transports publics qui permet de gérer cette fonctionnalité).

En cas d'incident de paiement, la mention « impayé » est inscrite dans la zone de commentaire de la base GFC. Cette indication est supprimée manuellement si le débiteur régularise sa situation. Dans le cas contraire, la mention « impayé » demeure inscrite sans limitation de durée et le client ne peut plus souscrire d'abonnement, à l'exception du passe anonyme.

Aucune information sur la possibilité d'être exclu de ce droit de souscrire un abonnement nominatif en raison d'un impayé n'est cependant portée à la connaissance des usagers lors de la conclusion des contrats.

2. La délégation s'est, ensuite, attachée à examiner les données de validation – date, heure et lieu de passage - transmises depuis les terminaux de validation associées aux numéros de carte, qui sont traitées dans une autre base de données que GFC. Les numéros de carte sont ensuite anonymisés dans un délai de 24 heures maximum.

Une copie de ces données de validation est conservée informatiquement dans une autre base avec un but statistique (définir les heures de pointes ou les périodes creuses, anticiper des événements majeurs tels que des manifestations, fêtes de la musique etc. sur la base de fréquentations ultérieures…). La délégation a constaté que les données de validation ne sont pas anonymisées dans cette base (le numéro de carte est conservé) et y figurent sans limitation de durée (les plus anciennes datent de la fin d'année 2007).

3. Puis, la délégation de la CNIL a examiné le dispositif de passe KORRIGO « anonyme », qui se présente, comme le passe nominatif, sous la forme d'une carte RFID. Il est en vente dans les agences commerciales, pour la somme de cinq euros, alors que le passe nominatif est gratuit. Il ne peut charger que des titres unitaires ou journaliers et non des abonnements (hebdomadaire, mensuel, annuel). Pour un utilisateur régulier, le passe anonyme revient donc, selon son âge, entre 2,5 et 4 fois le prix d'un abonnement nominatif.

La délégation de la CNIL a constaté une absence d'information sur ce type de passe, sur le site internet de la société, aux guichets de l'agence commerciale ou sur les supports papiers présentant les différents types d'abonnement. Depuis 2006, 53 passes anonymes ont été vendus pour 186 650 passes nominatifs.

4. S'agissant du traitement des réquisitions judiciaires, elles sont transmises à la société par télécopie, courriel ou courrier postal, dans le cadre d'enquêtes préliminaires, d'enquêtes de flagrance ou de commissions rogatoires. Aucun justificatif de la réquisition judiciaire n'est fourni en pièce jointe des courriels et la société ne procède à aucune authentification de l'expéditeur (si les adresses électroniques correspondent bien à des adresses « défense.gouv.fr » pour la gendarmerie nationale et « interieur.gouv.fr » pour la police nationale, ce type d'adresse peut cependant être détourné). Ces réquisitions sont traitées par le correspondant informatique et libertés de la société.

En réponse à ces réquisitions, les données de validation communiquées sont celles datant de moins de 24 heures et la société ne délivre pas de données de validation pour des trajets antérieurs. Les données sont envoyées aux demandeurs par une liaison non chiffrée.

Les données « clients » et « anciens clients » de GFC sont, quant à elles, conservées et communicables sans limitation de temps aux autorités de police, en l'absence de politique de conservation, de purge et d'archivage.

5. La délégation a constaté, concernant la sécurité des systèmes, que les mots de passe utilisés par le personnel pour accéder aux bases de données clients ou de données de validation étaient trop courts, qu'aucune formalisation des règles de sécurité du système d'information n'avait été faite par écrit. Il a été relevé que des mots de passe d'utilisateurs étaient écrits sur des papiers collés sur les écrans informatiques.

B. Procédure

A la suite de cette mission de vérification sur place, il a été décidé d'engager une procédure de sanction à l'encontre de la société, compte tenu de la nature et de la gravité des manquements constatés.

Le rapport du commissaire rapporteur, Mme Isabelle FALQUE-PIERROTIN, proposant à la formation restreinte de la CNIL de prononcer un avertissement, a été notifié à la société le 19 décembre 2008.

La société a formulé des observations écrites le 15 janvier 2009. Puis, représentée par M.C. et M. C., elle a présenté ses observations orales lors de la séance de la formation restreinte du 20 janvier 2009.

II. Motifs de la décision

A/ Sur le manquement au respect de la vie privée et des libertés individuelles

La Commission rappelle qu'en application de l'article 1er de la loi du 6 janvier 1978 modifiée : *« 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 ».*

La délibération n° 2008-161 du 3 juin 2008 portant autorisation unique (n° 15) 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 transports public, s'inspirant, ainsi, de l'article premier de la loi du 6 janvier 1978 précité, prévoit, dans son préambule, que « *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 ».*

La société a souscrit un engagement de conformité à l'autorisation unique n° 15 le 7 novembre 2008.

Le rapporteur a constaté qu'il existe de véritables obstacles à souscrire un passe KORRIGO anonyme. En effet, l'abonnement avec ce passe n'offre que la possibilité de le charger à

l'unité, ce qui est très contraignant et très coûteux pour un utilisateur régulier. En outre, à l'inverse du passe nominatif, le passe anonyme est payant et d'une valeur de cinq euros. Ainsi, le passe anonyme coûterait entre 2,5 et 4 fois plus cher que le passe nominatif, selon l'âge de l'utilisateur.

Dans sa réponse du 15 janvier 2009, la société a indiqué à la CNIL qu'il appartenait à la Communauté d'agglomération Rennes Métropole de fixer les tarifs et les conditions d'attribution d'un titre de transport, au terme d'une part, de l'article 10 de la convention de gestion et d'exploitation du réseau de transport public de voyageurs dans le périmètre des transports urbains de l'agglomération rennaise et d'autre part, de la délibération du Conseil de Rennes Métropole du 30 mars 2006.

Lors de la séance de la formation restreinte du 20 janvier 2009, la société a, tout d'abord, exposé à la Commission qu'un quart des utilisateurs des transports publics rennais voyageait anonymement via la billetterie papier, ce qui établirait selon elle que ceux-ci disposent d'un choix entre des titres nominatifs et des titres anonymes. Elle a, ensuite, informé la Commission que des échanges avaient eu lieu entre la société et la Communauté d'agglomération au sujet du passe anonyme et qu'une réflexion était en cours afin de mettre éventuellement en place des abonnements anonymes en sus des tickets à l'unité. Or, la société a exposé que si des abonnements anonymes étaient mis en œuvre, le statut des abonnés (étudiant, retraité…) ne pourrait pas être pris considération afin de fixer un tarif adéquat. En outre, le remboursement intégral ou partiel des titres (en cas de grève ou par l'employeur) serait impossible.

La Commission relève que le respect de la vie privée et de la liberté d'aller et venir anonymement implique, aux termes de l'autorisation unique n° 15, 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. La société ayant souscrit à cette autorisation unique ne pouvait ignorer cette prescription. Le surcoût que représente le passe anonyme et la disproportion entre la diffusion des deux types de passe Korrigo est à cet égard édifiante, seuls 53 passes anonymes ayant été vendus pour 186 650 passes nominatifs, au jour du contrôle. Aussi, malgré les démarches engagées par la société auprès de la Communauté d'agglomération Rennes Métropole afin d'examiner la possibilité d'étendre le passe anonyme aux abonnements, la Commission relève qu'il n'existe, aujourd'hui, aucun véritable choix entre les deux titres Korrigo et qu'en l'état, la mise en œuvre quasi exclusive d'un passe nominatif constitue un manquement à l'article 1er de la loi du 6 janvier 1978 et aux finalités figurant dans l'autorisation unique n° 15.

B/ Sur le manquement à l'obligation de définition d'une finalité déterminée, explicite et légitime du traitement

La Commission rappelle, en outre, qu'en application du 2° de l'article 6 de la loi n° 78-17 du 6 janvier 1978 modifiée, les données à caractère personnel *« sont collectées pour des finalités déterminées, explicites et légitimes et ne sont pas traitées ultérieurement de manière incompatible avec ces finalités »*.

Le rapporteur a constaté qu'une liste des personnes ayant résilié leur autorisation de prélèvement automatique, dénommée « clients en résiliation définitive PA », contenant les données des clients ayant résilié ce mode de paiement, était créée à partir du traitement GFC.

La société n'a répondu à ce sujet, ni dans son courrier du 15 janvier 2009, ni lors de la séance de la formation restreinte du 20 janvier suivant. Elle n'a, dès lors, pas établi que cette liste répondrait à une finalité déterminée, explicite et légitime au sens du 2° de l'article 6 précité.

C/ Sur le manquement à l'obligation de définir une durée de conservation des données

La Commission rappelle, ensuite, qu'en application du 5° de l'article 6 de la loi n° 78-17 du 6 janvier 1978, les données à caractère personnel doivent être *« 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 »*.

L'article 4 de l'autorisation unique n° 15 dispose que *« 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 (…)
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.
Les informations relatives à la gestion des impayés sont immédiatement retirées de la liste d'opposition dès régularisation des sommes dues ; à défaut de régularisation, elles seront conservées pendant au maximum deux ans à compter de l'inscription ».

Le rapporteur a constaté que toutes les données figurant dans la base Gestion des fiches clients étaient conservées sans limitation de durée (dont notamment les coordonnées bancaires, en cas de résiliation du prélèvement automatique et la mention « impayé », en cas d'incident de paiement non régularisé). Les données de validation non anonymisées figurant dans le serveur S3 sont, également, conservées pour une durée indéterminée.

La société a, dans son courrier de réponse, indiqué à la Commission qu'une purge manuelle des clients « inactifs » de plus de 25 mois avait été effectuée en janvier 2009 et qu'une purge de la mention « impayé » était programmée pour la fin de ce même mois. Concernant les données de validation non anonymisées, la société a indiqué avoir rencontré des problèmes techniques empêchant cette anonymisation, mais que cette situation était en voie de régularisation. La société a précisé, lors de la séance du 20 janvier 2009, que ce processus serait achevé dans un délai de 75 à 100 jours.

La Commission relève que les purges manuelles réalisées sont ponctuelles puisqu'elles visent à apurer les bases des clients « inactifs » et des mentions « impayé ». Or, aucune véritable politique de purge n'a été mise en œuvre par la société afin de veiller au respect des délais de conservation indiqués à l'article 4 de l'autorisation unique n° 15. En outre, la société n'a rien répondu quant à la conservation, dans une liste spécifiquement créée, des données bancaires des personnes ayant résilié leur prélèvement automatique.

Il résulte de ce qui précède que les faits précités constituent un manquement aux dispositions précitées.

D/ Sur le manquement à l'obligation d'information des personnes

- En premier lieu, la Commission rappelle que le I de l'article 32 de la loi n° 78-17 du 6 janvier 1978 dispose que le responsable du traitement doit informer la personne auprès de laquelle sont recueillies des données à caractère personnel la concernant des informations sur l'identité du responsable du traitement, la finalité de ce traitement, le caractère obligatoire ou facultatif des réponses, les destinataires, leurs droit d'accès, de rectification et, le cas échéant, d'opposition aux données les concernant ainsi que des transferts de données envisagés à destination d'un Etat non-membre de la Communauté européenne.

En outre, l'article 6 de l'autorisation unique n° 15 impose une double information du client susceptible d'être inscrit dans le traitement de gestion des impayés : lors de la conclusion du contrat d'abonnement, puis préalablement à l'inscription dans le fichier des impayés et de la mise en opposition du titre de transport.

La rapporteur a constaté que les clients de la société ne sont pas informés de l'existence de la fonctionnalité « gestion des impayés » de la base gestion des fiches clients.

La société a, dans son courrier du 15 janvier 2009, informé la CNIL de l'insertion sur le formulaire d'adhésion de la mention suivante : *« en cas de litige de paiement, si malgré des relances, le règlement n'est pas effectué, la STAR se réserve le droit de bloquer la carte KORRIGO* ».

Or, quand bien même l'insertion d'une telle mention serait satisfaisante, la double information exigée par l'autorisation unique n° 15 fait défaut.

- En second lieu, la Commission rappelle que l'article 6 alinéa 2 de l'autorisation unique n° 15 dispose que: *« la possibilité d'utiliser des titres de transports anonymes doit être portée à la connaissance des intéressés selon les mêmes modalités que celles prévues pour les titres de transports nominatifs »*.

Le rapporteur a constaté qu'aucune information n'était diffusée sur l'existence d'un passe anonyme sur le site internet www.star.fr et sur les supports papiers présentant les différents types d'abonnement. Une telle information n'est pas non plus accessible aux guichets des agences commerciales.

La société a, dans son courrier du 15 janvier 2009, informé la CNIL d'une part, qu'elle diffusait désormais à chaque guichet de l'agence commerciale, des supports d'information et une grille tarifaire mentionnant le passe anonyme ; d'autre part, que le site internet www.star.fr avait été actualisé pour intégrer des informations sur ce passe.

Si l'information diffusée sur la grille tarifaire est assez claire, en revanche, le site internet ne mentionne aucune information sur le passe anonyme dans la rubrique « *Titre, tarifs et points de vente* », qui présente tous les autres titres existants. Il est nécessaire de se rendre sur la page dédiée à Korrigo, afin de trouver en fin de document une mention courte, peu lisible et incomplète sur le passe anonyme. Ainsi, les supports d'information ne procèdent pas à une promotion égale des deux passes.

Il résulte de ce qui précède que les pratiques commerciales de la société, qui consistent à favoriser l'information portant sur le passe nominatif et à ne pas présenter le passe anonyme selon les mêmes modalités, ne sont pas conformes aux dispositions précitées.

E/ Sur le manquement à l'obligation de sécurité et de confidentialité des données

La Commission rappelle enfin que l'article 34 de la loi n° 78-17 du 6 janvier 1978 dispose que « *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* ».

Le rapporteur a constaté que les postes de travail n'étaient pas suffisamment protégés et que les utilisateurs n'étaient pas sensibilisés aux règles de sécurité : mots de passe trop courts non conformes aux recommandations de la Commission, qui préconise d'adopter des identifiants composés de huit caractères alphanumériques, non triviaux et renouvelés régulièrement ; mots de passe écrits sur des papiers collés sur les écrans informatiques et absence de formalisation par écrit des règles de sécurité du système (défaut de politique de sécurité, de procédures pratiques ou de charte utilisateur). Il a, également, été constaté que les réponses aux réquisitions judiciaires étaient envoyées par courriels sans authentification des auteurs de ces courriels et que les données de validation transmises n'étaient pas cryptées.

La société, dans sa réponse du 15 janvier 2009, a indiqué à la CNIL avoir mis en place un accès sécurisé, par identifiant et mot de passe individuels, à la base Gestion des fiches clients ainsi qu'à la base WEBI relative à la gestion des statistiques. Deux notes ont été adressées aux utilisateurs des bases pour les sensibiliser sur l'utilisation des mots de passe. La société souhaite, également, instaurer une procédure interne des réquisitions judiciaires, dont le projet devra être validé par les officiers de police judiciaire, et mettre en place des certificats numériques pour garantir l'identité de l'expéditeur et le cryptage du contenu du mail.

La Commission constate que la politique de gestion des mots de passe mise en place est satisfaisante ainsi que le projet de certificats numériques pour les réquisitions judiciaires.

Elle relève cependant que les règles de sécurité du système d'information n'ont pas été formalisées par écrit au moyen d'une politique de sécurité, de procédures pratiques ou de charte utilisateur. Les deux notes de liaison ne constituent pas une sensibilisation des utilisateurs suffisante.

Ainsi, les garanties apportées par la société en terme de sécurité des données sont insuffisantes au regard de l'article 34 précité.

Sur les manquements constatés

Il résulte de ce qui précède, eu égard aux manquements constatés relatifs au respect de la vie privée et à la liberté d'aller et venir, à la finalité du traitement, à la durée de conservation des données, à l'information des personnes et à la sécurité et la confidentialité des données, que la société KEOLIS RENNES verra prononcer à son encontre un avertissement.

Sur la publicité de la délibération

Eu égard à la nature et à la gravité des manquements commis ainsi qu'à la nécessité, d'une part, pour les personnes physiques de connaître les règles relatives à la protection de leurs

données à caractère personnel et, d'autre part, pour les responsables de traitement de mieux appréhender les règles qui s'imposent à eux, la délibération de la Commission sera rendue publique sur le site internet de la CNIL et sur le site internet Légifrance.

PAR CES MOTIFS

Conformément aux articles 45 et suivants de la loi du 6 janvier 1978 modifiée, la formation restreinte de la CNIL, après en avoir délibéré, décide de :

- **prononcer un avertissement à l'encontre de la société KEOLIS RENNES ;**
- **publier la présente décision sur le site internet de la CNIL et sur le site Légifrance.**

Le président

Alex TÜRK

La société KEOLIS RENNES dispose d'un délai de deux mois à compter de la notification de la présente décision pour exercer à son encontre un recours devant le Conseil d'Etat.