Études de cas

Géolocalisation de véhicules d'entreprise

Date	:	17 mars 2017
Statut	:	Approuvé
Classification	:	Public
Nombre de pages	:	11
Responsable des travaux	:	Matthieu GRALL
Validation	:	Groupe de travail
Approbation	:	Conseil d’administration

Ce document a été réalisé par le Club EBIOS

Responsable des travaux :

- CNIL (Matthieu GRALL)

Contributeurs :

- BSSI (Ludovic LECOMTE)
- BULL SAS (Dominique CASTAN)
- Cyril PATRIGEON
- CGI BUSINESS CONSULTING (Franck YVELIN)

Sommaire

Introduction

Ce document présente une étude de cas de l'utilisation de la méthode EBIOS[1] pour gérer des risques sur la vie privée de personnes concernées par un traitement de données à caractère personnel. Seuls ces risques sont étudiés.

Le contexte est celui d'une entreprise française dont l'employeur souhaite équiper les véhicules de fonction de ses commerciaux de dispositifs de géolocalisation[2]. Son but est essentiellement d'optimiser leurs déplacements pour réduire les coûts associés, dans la mesure où il a la charge d'organiser leurs déplacements[3] de manière individuelle.

En effet, l'employeur a constaté les limites des dispositifs de planification standards individuels. Ils ne permettent pas de planifier des itinéraires complexes d'un seul véhicule, et encore moins d'un parc complet. Il n'est donc pas possible d'optimiser les déplacements des commerciaux dans leur ensemble. En outre, ils ne mesurent que la position du véhicule et ne considèrent pas la durée d'utilisation du véhicule, le kilométrage parcouru ou les vitesses de circulation, ce qui limite les possibilités d'optimisation. Le service associé doit donc permettre cette optimisation d'itinéraires.

L'étude des risques a pour objectif de déterminer des modalités de mise en œuvre respectueuses de la vie privée de ses employés.

En effet, l'enjeu de l'employeur réside dans l'acceptation du traitement par les commerciaux, qui pourraient contester la proportionnalité du dispositif ou estimer qu'ils doivent avoir une liberté dans leurs déplacements.

L'employeur : *Comment faire en sorte que mes commerciaux ne se sentent pas « fliqués » ? Comment prouver à mes employés que seules des données professionnelles sont collectées ?*

Un commercial : *Puis-je me faire licencier pour avoir utilisé mon véhicule de fonction à des fins personnelles ? Qu'en est-il de ma liberté de déplacement ?*

La CNIL : *Le dispositif n'est-il pas disproportionné ?*

[1] Expression des besoins et identification des objectifs de sécurité. Méthode de gestion des risques de l'Agence nationale de la sécurité des systèmes d'information (ANSSI).

[2] Lorsqu'on parle de géolocalisation il serait plus juste de parler de « chronogéolocalisation ». Ce qui est recherché n'est pas seulement où était la personne mais où était la personne tel jour à telle heure. Si elle n'est pas forcément recherchée en temps réel, il s'agit bien d'un suivi dans le temps et dans l'espace des déplacements (traces).

[3] On rappelle qu'il est interdit de géolocaliser un employé disposant de manière certaine d'une liberté dans l'organisation de ses déplacements (visiteurs médicaux, VRP…).

1 Le contexte : géolocalisation de véhicules de commerciaux pour optimiser les itinéraires

L'étude a tout d'abord consisté à décrire le contexte, c'est-à-dire le traitement (sa finalité, son fonctionnement, ses enjeux), les données à caractère personnel[4], les supports sur lesquels elles reposent, les sources de risques[5] et les références à considérer (lois, règlements, procédures…).

Le traitement a pour finalité d'optimiser les itinéraires des commerciaux dans le cadre de leurs tournées, afin de réduire leur longueur et leur coût en carburant.
Fonctionnellement, il comprend la planification des visites de clients et prospects par les commerciaux, le suivi du parcours de leurs véhicules et la recherche d'optimisations. Il doit donc permettre d'étudier les parcours de chaque commercial et de fournir des statistiques exploitables concernant l'ensemble des commerciaux pour mesurer l'atteinte des objectifs.
Une finalité accessoire est d'assurer le suivi du temps de travail des commerciaux, qui ne peut être réalisé par d'autres moyens.
Le principal enjeu réside dans l'augmentation des profits (possibilité de réaliser plus de visites et donc plus de ventes, réalisation d'économies en termes de carburant).

S'agissant des données à caractère personnel, ce sont les données de géolocalisation associées à chaque véhicule, lui-même affecté à un commercial.

Concernant les supports, il est prévu que le traitement repose sur un boîtier GPS embarqué dans les véhicules. Ce boîtier communiquerait par GSM avec un serveur hébergé chez un prestataire, qui stockerait également les données collectées dans une base de données. On note que le boîtier lui-même peut stocker temporairement des données (quelques jours au maximum) pour palier aux soucis de captation du réseau (tunnel, zone peu couverte) ou aux soucis de sur-taxation de la communication (zones frontalières). L'employeur accèderait à une application du prestataire via Internet, afin de gérer le lien entre les véhicules et les commerciaux, de paramétrer le boîtier (horaires, alertes sur zone géographique…) et de visualiser les données. Des tableaux de bord lui seraient envoyés une fois par mois par courrier électronique.

Mesures existantes identifiées
L'accès à l'application web du prestataire (et donc à la base de données) serait contrôlé par un identifiant et un mot de passe.
Les processus légaux ne sont pas encore fixés. L'étude devra justement contribuer à les définir.

Dans ce cadre, les principales références à considérer sont les suivantes :
- ✓ la [Fiche-Geoloc] et la [NS51] ;
- ✓ la fiche n°10 du [Guide-Employeur][6] et la [Fiche-GSM-GPS] ;
- ✓ le Code du travail (proportionnalité, consultation des instances représentatives…) ;
- ✓ le Code de la route (limitations de vitesse…).

Dans le contexte étudié, les sources de risques les plus plausibles sont les suivantes :
- ✓ l'employeur ;
- ✓ le prestataire (en tant qu'exploitant/administrateur) ;
- ✓ les commerciaux ;
- ✓ des concurrents de l'entreprise ;
- ✓ les tiers intervenant sur les véhicules (installateur, garagiste…) ;
- ✓ les forces de l'ordre.

[4] Dont la compromission, la modification ou la disparition pourrait entraîner un préjudice pour les personnes concernées.

[5] Qui peuvent être à l'origine des menaces.

[6] « Les dispositifs de géolocalisation GSM/GPS ».

2 Les risques : des atteintes potentiellement graves à la vie privée des commerciaux

L'étude a ensuite consisté à déterminer les risques à partir des éléments précédemment identifiés, et à les estimer en termes de gravité et de vraisemblance, compte tenu des mesures prévues initialement. Le tableau suivant présente les exemples les plus pertinents de cette appréciation des risques :

Risques	Événements redoutés jugés comme les plus graves (impacts sur les personnes concernées)	Mesures réduisant la gravité	Gravité	Menaces jugées comme les plus vraisemblables	Vulnérabilités	Capacités des sources de risques	Mesures réduisant la vraisemblance	Vraisemblance maximale
R1 – Accès illégitime à des données par l'employeur	La vie privée des commerciaux est atteinte par « flicage » en dehors du temps de travail (déjeuners, soirées, week-end, vacances).	Aucune	3. Importante	L'employeur pourrait détourner l'usage de l'application pour accéder à des données dont il n'est pas censé devoir prendre connaissance.	Maximales (les fonctionnalités de l'application peuvent le permettre)	Limitées (l'employeur souhaite une solution respectueuse de la vie privée)	Aucune	3. Importante
R2 – Accès illégitime à des données par un concurrent ou un tiers intervenant sur les véhicules	Un concurrent ou un tiers récupère les données (professionnelles et personnelles) pour « voler » la clientèle de l'entreprise.	Aucune	3. Importante	Un concurrent ou un tiers pourrait détourner l'usage de l'application pour accéder à des données dont il n'est pas censé devoir prendre connaissance.	Limitées (une intrusion informatique est nécessaire, même si cette intrusion est plus facile pour un tiers intervenant sur les véhicules)	Négligeables (des concurrents pourraient être intéressés par les données)	Contrôle d'accès par identifiant et mot de passe	1. Négligeable
R3 – Accès illégitime à des données par un administrateur informatique du prestataire	Un administrateur du prestataire récupère les données pour les vendre ou faire du chantage.	Aucune	3. Importante	Un administrateur pourrait directement accéder à la base de données.	Maximales (les données sont accessibles aux administrateurs)	Importantes (il n'est pas exclu qu'un administrateur puisse et veuille le faire)	Charte	3. Importante
R4 – Disparition accidentelle de données	Les commerciaux sont accusés d'avoir manipulé le dispositif.	Aucune	2. Limitée	Un dysfonctionnement ou une panne pourrait avoir lieu.	Limitées	Limitées	Aucune	2. Limitée
R5 – Disparition délibérée de données	Les commerciaux sont accusés d'avoir manipulé le dispositif.	Aucune	2. Limitée	Un commercial pourrait utiliser une plaque en métal pour brouiller les ondes, ou débrancher le dispositif.	Importantes (le dispositif est manipulable)	Limitées (le dispositif est facilement accessible, mais il est peu probable que les commerciaux le manipulent)	Aucune	2. Limitée
R6 – Modification non désirée de données	Le dispositif ne permet par aux commerciaux d'optimiser leur itinéraire, ce qui pourrait leur être reproché par l'employeur.	Aucune	2. Limitée	Une erreur de manipulation ou de mise à jour du logiciel, ou un sinistre lié à un logiciel malveillant pourrait se produire.	Limitées	Limitées	Aucune	2. Limitée

Une cartographie a été réalisée pour les risques dont la gravité est élevée et très élevée (voir le schéma en fin d'étude).

3 Les mesures : un dispositif respectueux de la vie privée

Les principales mesures sont présentées ici. Elles doivent non seulement permettre de traiter les risques, mais aussi de respecter les principes fondamentaux de la protection de la vie privée[7]. L'objectif visé est notamment d'éviter que :

- les commerciaux ne soient pas convenablement informés (affichage au siège de l'entreprise alors que les commerciaux n'y vont jamais, dispositif installé sans préciser pourquoi, information orale, ou pas individuelle…), et donc géolocalisés à leur insu ;
- des données non pertinentes ou excessives par rapport à la finalité soient collectées (ex : enregistrement de la vitesse instantanée ou maximale, détection de dépassement de 130km/h) ;
- les données soient utilisées pour une autre finalité que celle prévue (ex : licenciement), en permettant à l'employeur de détourner l'usage de l'application pour corréler les données prévues avec d'autres informations telles que les zones géographiques et les limitations de vitesse associées ;
- les forces de l'ordre exploitent les données pour sanctionner des excès de vitesse.

Des données limitées

Ne jamais collecter plus de données que les suivantes (cf. [NS51]) :

- identification de l'employé : nom, prénom, coordonnées professionnelles, matricule interne, numéro de plaque d'immatriculation du véhicule ;
- données relatives aux déplacements des employés : données de localisation issues de l'utilisation d'un dispositif de géolocalisation, historique des déplacements effectués ;
- données complémentaires associées à l'utilisation du véhicule : vitesse de circulation du véhicule[8], nombre de kilomètres parcourus, durées d'utilisation du véhicule, temps de conduite, nombre d'arrêts.

Cette mesure contribue à respecter les principes fondamentaux et à réduire la gravité des risques R1, R2 et R3.

Une destruction des données en fin de durée de conservation

Déterminer et appliquer une procédure pour détruire les données au bout de leur durée de conservation. Celle-ci ne doit pas excéder deux mois sauf si :

- « *une réglementation spécifique le prévoit ;*
- *une telle conservation est rendue nécessaire à des fins de preuve de l'exécution d'une prestation, lorsqu'il n'est pas possible de rapporter cette preuve par un autre moyen. Dans ce cas, la durée de conservation est fixée à un an, cette durée ne faisant pas obstacle à une conservation supérieure en cas de contestation des prestations effectuées ;*
- *la conservation est effectuée pour conserver un historique des déplacements à des fins d'optimisation des tournées, pour une durée maximale d'un an. Dans le cadre du suivi du temps de travail, seules les données relatives aux horaires effectués peuvent être conservées pendant une durée de cinq ans* » (cf. [NS51]).

Pour ce faire :

- stockage des courriers électroniques dans une boîte dédiée ;
- nettoyage de la boîte par l'employeur chaque semaine.

Quant aux données de journalisation, elles « *doivent être conservées pendant une durée de six mois* » (cf. [NS51]).

Cette mesure contribue à respecter les principes fondamentaux et à réduire la gravité des risques R1, R2 et R3.

[7] Finalité déterminée, explicite et légitime ; données adéquates, pertinentes et non excessives ; durées de conservation limitées ; information des personnes ; droits d'accès, de rectification, etc. (cf. [Loi-I&L]).

[8] Vitesse moyenne pour que les infractions éventuelles ne puissent pas être identifiées et éviter « *le traitement de la vitesse maximale* » (cf. [NS51]).

Une information des commerciaux

Informer les commerciaux « *préalablement à la mise en œuvre du traitement :*
- *de l'identité du responsable de traitement ou de son représentant ;*
- *de la finalité poursuivie par le traitement ;*
- *des destinataires ou catégories de destinataires des données ;*
- *de l'existence d'un droit d'accès aux données les concernant, d'un droit de rectification et d'un droit d'opposition pour motif légitime, ainsi que des modalités d'exercice de ces droits* » (cf. [NS51]).

Pour ce faire :
- formaliser une note de service[9] et la présenter individuellement aux commerciaux par le responsable hiérarchique ;
- placer une mention d'information dans l'habitacle des véhicules (cela dissuade aussi du vol).

Cette mesure contribue à respecter les principes fondamentaux et à réduire la vraisemblance du risque R5.

Un accès aux données par les commerciaux

Permettre aux commerciaux l'accès aux données issues du dispositif de géolocalisation le concernant en s'adressant au service ou à la personne qui lui aura été préalablement indiqué.
Pour ce faire :
- accès aux paramètres du dispositif en ligne ;
- demande directe à l'employeur.

Cette mesure contribue à respecter les principes fondamentaux et à réduire la vraisemblance des risques R1 et R5.

L'exercice du droit de rectification

Permettre l'exercice du droit de rectification, notamment en cas de départ ou de changement d'affectation (suppression de la base).
Cette mesure contribue à respecter les principes fondamentaux et à réduire la vraisemblance des risques R1 et R5.

Une charte comme engagement de l'employeur et des employés

S'engager à ce que la finalité du traitement consiste bien en « *une meilleure allocation des moyens pour des prestations à accomplir en des lieux dispersés* » (cf. [NS51]).
Pour ce faire :
- rédiger une charte formalisant l'ensemble des mesures que l'employeur et les employés doivent s'engager à respecter ;
- faire signer cette charte par l'employeur et par chaque employé.

Cette mesure contribue à respecter les principes fondamentaux et à réduire la vraisemblance du risque R5.

La consultation des instances représentatives du personnel

Procéder « *à l'information et à la consultation des instances représentatives du personnel avant la mise en œuvre d'un dispositif de géolocalisation des employés* » (cf. [NS51]).
Pour ce faire :
- réaliser la présente étude ;
- formaliser la note de service ;
- formaliser la charte ;
- obtenir leur validation des représentants du personnel.

Cette mesure contribue à la conformité à la [NS51].

[9] Toutefois, il est inutile d'obtenir le consentement dans le cadre d'une relation employé-employeur. Par ailleurs, une opposition n'est possible qu'en cas d'absence d'information ou de déclaration. La note devrait préciser que la tenue des objectifs commerciaux ne sera pas en conflit avec le respect du code de la route.

Des exigences sur l'offre de service

Choisir une offre qui permette :

- de ne réaliser que le traitement de la vitesse moyenne pour que les infractions éventuelles ne puissent pas être identifiées et éviter « *le traitement de la vitesse maximale* » (cf. [NS51]) ;
- de savoir quand le système est actif (voyant lumineux ou sonore) ;
- un paramétrage par l'employeur des plages horaires où le système est actif, accessible en lecture par les commerciaux sans que des comptes individuels ne soient créés ;
- de ne pas faire apparaître les données en dehors des horaires de travail ;
- la désactivation du système sur le boîtier ou dans les paramétrages par les commerciaux, qui « *doivent avoir la possibilité de désactiver la fonction de géolocalisation des véhicules, en particulier à l'issue de leur temps de travail ou pendant leurs temps de pause* » (cf. [NS51]) ; en outre, « *les employés investis d'un mandat électif ou syndical ne doivent en aucun cas faire l'objet d'une opération de géolocalisation lorsqu'ils agissent dans le cadre de l'exercice de leur mandat* » (cf. [NS51]) ;
- limiter l'accès aux données de géolocalisation aux « *personnes en charge de coordonner, de planifier ou de suivre les interventions, les personnes en charge de la sécurité des biens transportés ou des personnes ou, le cas échéant, le responsable des ressources humaines* » par « *un mécanisme de gestion des habilitations, régulièrement mis à jour* » (cf. [NS51]) ;
- de contrôler les accès individuels aux données de géolocalisation « *par un identifiant et un mot de passe individuels respectant les recommandations de la Commission et régulièrement renouvelé, ou par tout autre moyen d'authentification garantissant au moins le même niveau de sécurité* » (cf. [NS51]) ;
- de mettre en œuvre « *une traçabilité, dont l'intégrité est assurée, afin de permettre la détection d'éventuelles tentatives d'accès frauduleux ou illégitimes, en incluant un horodatage, l'identifiant de l'utilisateur, ainsi que l'identification des données concernées, et ceci pour les accès en consultation, modification ou suppression. Les données de journalisation doivent faire l'objet d'une revue régulière visant à identifier tout incident de sécurité* » (cf. [NS51]) ;
- de protéger les informations transmises via Internet par « *des mesures adéquates permettant de garantir la confidentialité des données échangées, telles qu'un chiffrement des données* » (cf. [NS51]).

Cette mesure contribue à respecter les principes fondamentaux et à réduire la vraisemblance de tous les risques.

Des engagements contractuels

Préciser dans le contrat avec le prestataire :

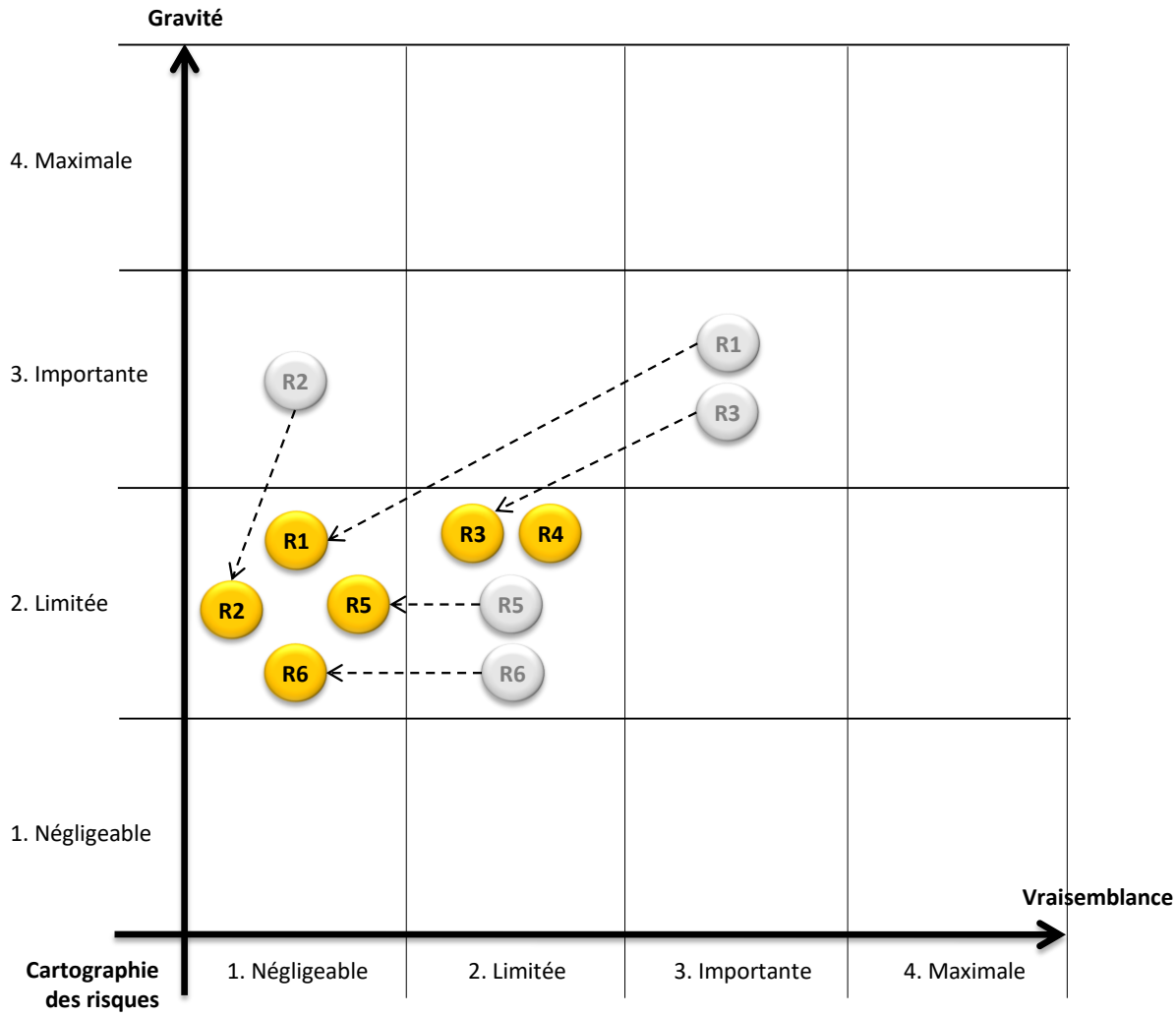
- la finalité poursuivie par le traitement de géolocalisation ;
- les engagements de qualité de service concernant la disponibilité, l'intégrité et la confidentialité des données traitées, ainsi que la « *mise à jour des mesures de sécurité au regard de la réévaluation régulière des risques* » (cf. [NS51]) ;
- le fait qu'il s'engage à respecter les normes et les obligations la [Loi-I&L] ;
- le fait qu'il s'engage à faire réaliser un audit de sécurité par un organisme indépendant et à tenir les résultats à disposition de l'employeur.

Cette mesure contribue à respecter les principes fondamentaux et à réduire la vraisemblance de tous les risques.

Une formalité auprès de la CNIL

Réaliser une déclaration de conformité à la [NS51] auprès de la CNIL.
Cette mesure contribue à respecter les principes fondamentaux.

Les risques sont ré-estimés en tenant compte de ces mesures, afin d'évaluer les risques résiduels :



Bien que la gravité des risques demeure non négligeable, puisqu'ils restent préjudiciables pour les commerciaux, les mesures prévues permettent de réduire la vraisemblance à un niveau minimal ou limité.

En outre, le bénéfice attendu par l'employeur, et partagé par les commerciaux qui pensent que l'optimisation des itinéraires peut être utile à l'atteinte de leurs objectifs, doit permettre de rendre ces risques acceptables.

Les risques résiduels sont donc considérés comme pouvant être pris.

Conclusion

Cette étude de cas montre que la méthode EBIOS peut être employée très simplement pour étudier les risques sur la vie privée.

Annexes

Glossaire

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. Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne. [Loi-I&L]
Traitement de données à caractère personnel (traitement)	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, et notamment la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction. [Loi-I&L]

Bibliographie

Les références suivantes apparaissent entre crochets dans le présent document.

[Loi-I&L]	Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés[10].
[Fiche-Geoloc]	Fiche pratique « Une recommandation destinée à encadrer la géolocalisation des véhicules des employés », 27 avril 2006, CNIL.
[NS51]	Norme simplifiée n° 51 : Délibération n°2015-165 du 4 juin 2015 portant adoption d'une norme simplifiée concernant les traitements automatisés de données à caractère personnel mis en œuvre par les organismes publics ou privés destinés à géolocaliser les véhicules utilisés par leurs employés.
[Guide-Employeur]	Guide pour les employeurs et les salariés, 2010, CNIL.
[Fiche-GSM-GPS]	Fiche pratique « Les dispositifs de géolocalisation GSM/GPS », CNIL.
[EBIOS]	*Expression des Besoins et Identification des Objectifs de Sécurité – EBIOS – Méthode de gestion des risques*, 25 janvier 2010, ANSSI.

[10] 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 et par la loi n° 2009-526 du 12 mai 2009 de simplification et de clarification du droit et d'allègement des procédures.