Projet de recommandation

Utilisation des données de localisation des véhicules connectés

Version soumise à consultation jusqu'au
20 mai 2025

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

Table des matières

1. Introduction

1. Les modes de transport (voitures, scooters, vélos, etc.) et leurs utilisateurs génèrent une quantité croissante de données. Celles-ci peuvent être produites directement par les équipements et systèmes du véhicule, mais également par des équipements embarqués (par exemple, un boîtier télématique) ou les appareils connectés du conducteur et des passagers (téléphone mobile multifonctions, tablette, etc.).

2. L'exploitation de ces données permet, par exemple, de proposer des services innovants pour les usagers des transports permettant des gains de sécurité, une amélioration de l'expérience du déplacement (info-divertissement, confort, maintenance, etc.) ou encore une optimisation de l'organisation du déplacement. Dans le même temps, la connectivité des véhicules implique le recueil de données susceptibles de toucher à la vie privée de l'individu (déplacements, comportement au volant, etc.).

3. Parmi ces données, la localisation apparait comme une donnée centrale pour la plupart des acteurs de l'écosystème du véhicule connecté. Les données de localisation sont considérées comme des données hautement personnelles[1], particulièrement intrusives pour la vie privée des personnes, puisqu'elles sont susceptibles de révéler leurs déplacements, leurs lieux de fréquentation ou encore, leurs centres d'intérêts.

4. Tel que souligné dans les lignes directrices 01/2020 du comité européen de la protection des données (CEPD)[2], l'utilisation de technologies de localisation appelle la mise en œuvre de garanties spécifiques, conformément au règlement général de protection des données (RGPD).

5. Cette recommandation, élaborée en concertation avec les acteurs du véhicule connecté a pour objectif de rappeler les règles applicables en matière de traitement des données de localisation dans le contexte du véhicule connecté et d'émettre des recommandations concrètes pour s'y conformer.

6. Elle se concentre sur les usages de véhicules connectés par des particuliers, en tant que propriétaires ou locataires.

Les différents véhicules concernés

[1] Le Comité européen de la protection des données (CEPD) dans ses lignes directrices du 4 octobre 2017, considère les données de localisation comme étant des « *données à caractère hautement personnel* ». Il estime que ces données sont considérées comme sensibles, au sens commun du terme, dans la mesure où elles ont un impact sur l'exercice d'un droit fondamental. En effet, la collecte des données de localisation met en cause la liberté de circulation.

[2] Lignes directrices 01/2020 sur le traitement des données à caractère personnel dans le contexte des véhicules connectés et des applications liées à la mobilité (voir en ce sens le point 45), CEPD, URL : https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-012020-processing-personal-data-context_fr).

2. Périmètre de la recommandation

Comment lire cette recommandation ?

Cette **recommandation vise à rappeler les obligations** posées par la règlementation (par exemple, « le responsable du traitement doit ») et **formuler des recommandations** pour s'y conformer (par exemple, « la CNIL recommande »). Il est possible que les responsables de traitement identifient des manières alternatives de se conformer à leurs obligations et doivent alors être en mesure de justifier leur choix. Certains éléments sont également formulés à titre de bonnes pratiques et permettent d'aller plus loin que le respect de la règlementation (par exemple, « A titre de bonnes pratiques, la CNIL encourage »).

2.1 À qui s'adresse cette recommandation ?

7. La recommandation s'adresse à l'ensemble des acteurs du véhicule connecté, et plus particulièrement :

- aux **constructeurs** ;
- aux **gestionnaires de flotte**, acteurs privés ou publics, qui proposent des véhicules (voitures, scooters, cycles, trottinettes etc.) en location courte[3] ou en location longue durée[4] ;
- aux **fournisseurs** d'outils de télématiques, tels que notamment des boîtiers, qui sont installés sur les véhicules ;
- aux **agrégateurs et intégrateurs de données**, qui peuvent notamment intervenir comme intermédiaires entre les constructeurs de véhicules et d'autres acteurs afin d'organiser la transmission des données liées aux véhicules.

8. La recommandation se concentre sur les **usages de véhicules connectés par des particuliers**, en tant que propriétaire ou locataire. Elle ne couvre pas l'utilisation de véhicules de fonction mis à disposition de salariés par leur employeur[5].

2.2 Qu'est-ce qu'une donnée de localisation ?

9. Les données de localisation correspondent aux **données permettant de déterminer la localisation d'un objet ou d'une personne avec une certaine précision**, le plus souvent en s'appuyant sur un système de géo-positionnement par satellite (par exemple, le système européen Galileo ou le système états-unien GPS).

Données de localisation et données de géolocalisation : quelle différence ?

La localisation d'un individu ou d'un objet regroupe l'ensemble des techniques permettant de savoir où il se trouve. La localisation d'un individu peut être absolue ou relative (c'est-à-dire une position par rapport à un autre objet dont la position est connue).

La géolocalisation est un sous-ensemble des techniques de localisation permettant de positionner cet individu ou cet objet sur une carte ou un plan grâce à ses coordonnées géographiques. Ces coordonnées géographiques sont souvent représentées sous la forme d'une latitude, d'une longitude et parfois d'une altitude.

Les coordonnées géographiques décrivant la position d'un individu ou d'un objet peuvent être plus ou moins précises : en général une précision de quelques mètres ou généralisées pour n'inclure que le quartier d'une ville, voire la ville, le département ou le pays de l'individu ou de l'objet. La précision des coordonnées géographiques dépend également de la technologie utilisée pour le géo-positionnement.

[3] Pour les besoins de la recommandation, la location courte répond à un besoin ponctuel, pour une durée allant de quelques minutes à plusieurs mois, généralement facturée en fonction de cette durée.

[4] Pour les besoins de la recommandation, la location longue s'étale sur une année ou plus, généralement facturée sous forme de mensualités.

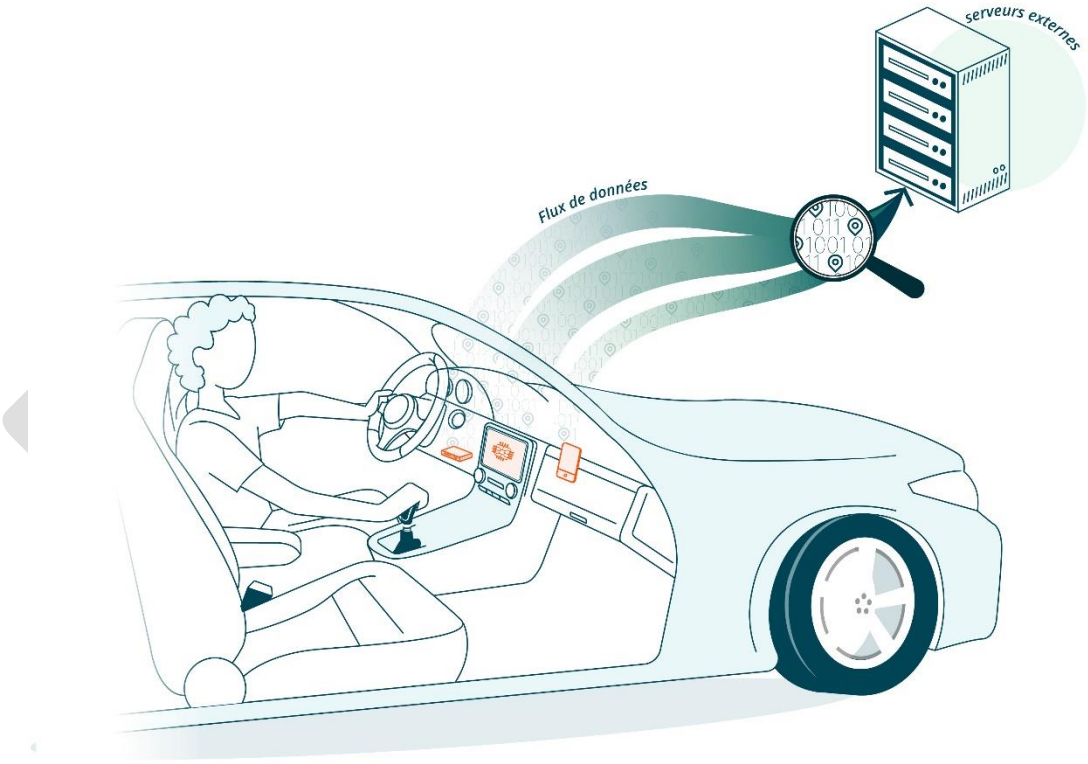
[5] Des informations relatives à la localisation des salariés figurent sur le site de la CNIL : « La géolocalisation des véhicules de salariés », URL : https://www.cnil.fr/fr/la-geolocalisation-des-vehicules-des-salaries.

Les sources des données de localisation

10. Les données de localisation des véhicules connectés peuvent être obtenues de différentes manières, selon les acteurs :

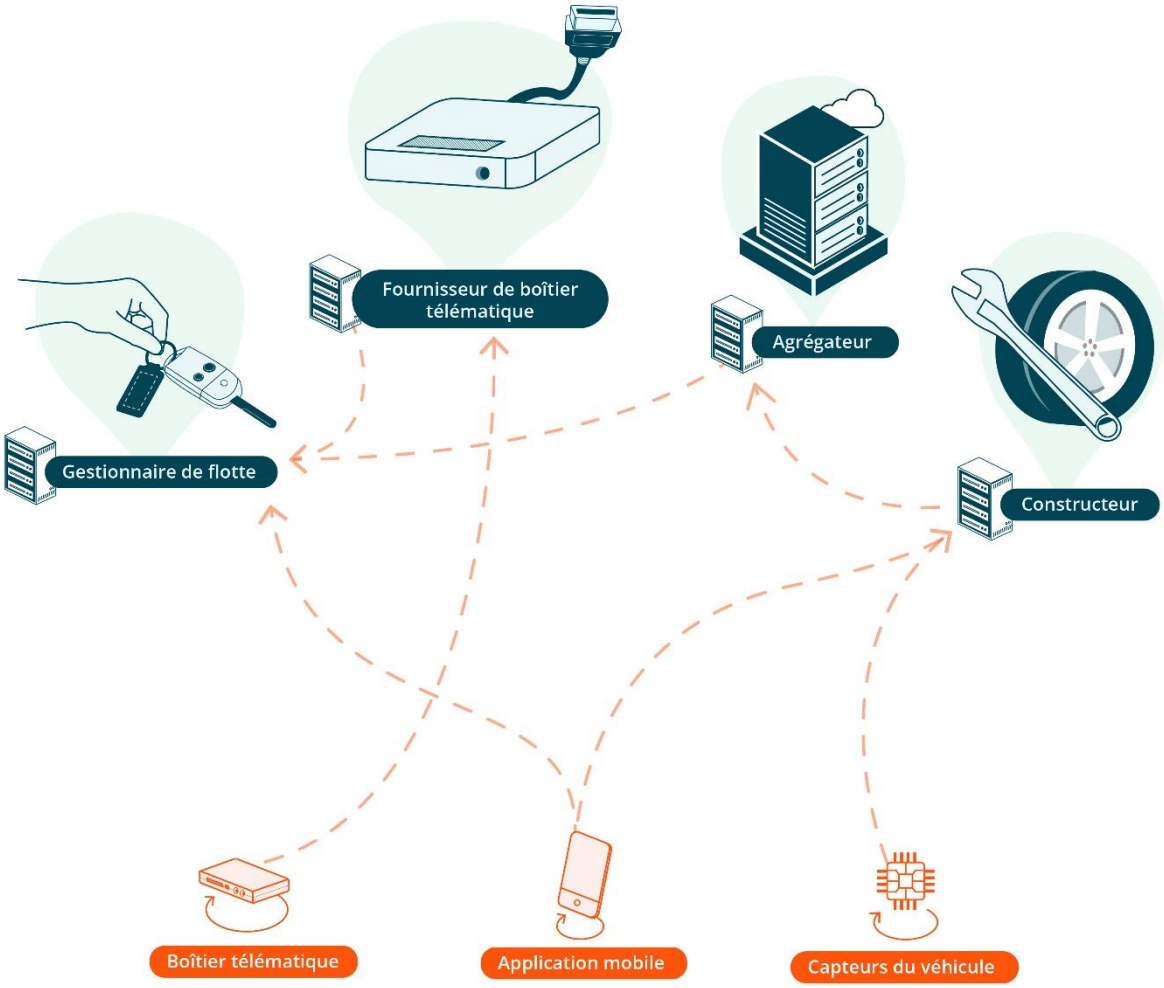
- elles peuvent être **collectées directement au sein du véhicule,** par le biais d'un ou plusieurs dispositifs intégrés par le constructeur (tels qu'un capteur GPS) ou par le biais d'un outil de télématique (intégré au véhicule ou ajouté postérieurement), tel qu'un boîtier, généralement branché au port de diagnostic du véhicule (ou port « *on board diagnostics* », dit port OBD) ;
- elles peuvent être collectées **par le biais d'une application pour téléphone mobile** fournie par le loueur ou le constructeur du véhicule ;
- une fois collectées, elles peuvent être **mises à disposition par le biais d'une interface de programmation d'application (API)**, telles que les API des constructeurs ;
- elles peuvent être **obtenues, parfois, uniquement par le biais d'un intégrateur, ou d'un agrégateur de données,** qui agit en tant qu'intermédiaire entre un constructeur de véhicules connectés et les acteurs souhaitant accéder aux données de ces véhicules. Dans certains cas, cet accès se fait après avoir effectué un travail sur les données fournies par le constructeur, tel que le tri, l'agrégation, l'anonymisation des données, etc.

Les différentes sources de données et leurs flux



CNIL.

Les différents acteurs et leurs flux de données.



LÉGENDE

Flux de données *Traitements en local*

Utilisations des données de localisation

11. La CNIL a identifié les principales finalités qui impliquent la collecte et le traitement de données de localisation des véhicules connectés.

12. Ces finalités font l'objet de recommandations spécifiques en partie 5 de la recommandation :

- **gestion de la flotte par les sociétés de location de véhicule** (gestion de l'exécution des contrats de location ainsi que la performance de leur service) ;
- **assistance aux personnes et dépannage du véhicule ;**
- **assistance aux personnes en cas d'accident** ;
- **lutte contre le vol ;**
- **optimisation et amélioration des produits et services** (identification des axes d'amélioration des équipements ou des services proposés).

Point d'attention

Un responsable du traitement peut collecter et traiter des données de localisation pour d'autres finalités, non couvertes par la recommandation.

Il lui appartiendra de mener sa propre analyse afin de vérifier que le traitement qu'il souhaite mettre en œuvre est conforme aux exigences du RGPD.

3. Recommandations générales

3.1 Respecter la règlementation applicable en matière de protection des données personnelles

Applicabilité du RGPD

13. Les données du véhicule connecté sont des données personnelles dès lors qu'elles se rapportent à une personne physique identifiée ou identifiable.

14. C'est notamment le cas des données de localisation du véhicule, dès lors que le véhicule peut être rattaché à une personne physique, qui peut être le propriétaire (par le biais du numéro d'identification du véhicule (VIN)[6], du certificat d'immatriculation ou du contrat d'assurance), ou le locataire (par le biais d'un contrat de location) du véhicule. Les données peuvent encore être rattachées à la personne qui s'est identifiée dans le système d'info-divertissement ou y a connecté son téléphone mobile multifonctions.

15. Par conséquent, le RGPD a vocation à s'appliquer aux traitements de ces données[7].

Point d'attention

Certains traitements de données sont effectués par des personnes physiques dans le cadre d'une activité strictement personnelle ou domestique et ne relèvent pas du RGPD (considérant 18 du RGPD). Il s'agit notamment de l'utilisation de données personnelles à l'intérieur des véhicules par les seules personnes concernées qui ont fourni ces données dans le tableau de bord du véhicule.

Toutefois, les dispositions du RGPD s'appliquent aux responsables du traitement ou aux sous-traitants qui fournissent les moyens de traiter des données personnelles pour de telles activités personnelles ou domestiques.

Ainsi, les acteurs (par exemple, le constructeur) sont, en principe, tenus de respecter les dispositions du RGPD pour les traitements des données qui y sont fournies par les personnes concernées, y compris si ces données ne sortent pas du véhicule.

Dans certains cas, ils ne seront pas soumis au RGPD malgré le fait qu'ils fournissent les moyens de traitement de données personnelles. Deux critères doivent être pris en compte :

- le traitement est initié à la discrétion de la personne, opéré sous son contrôle et pour son seul compte, c'est-à-dire décidé et mis en œuvre par cette dernière ;
- le traitement est réalisé dans un environnement cloisonné, c'est-à-dire sans intervention possible du tiers sur ces données : le tiers a fourni les moyens du traitement, mais il ne peut plus agir en aval sur les données.

16. Le RGPD ne s'applique pas lorsque la localisation du véhicule ne se rapporte pas à une personne physique identifiée ou identifiable.

Exemple

Les données de localisation des véhicules loués sont parfois collectées par des gestionnaires de flotte pour être en mesure d'assurer leur dépannage.

Lorsque la panne d'un véhicule survient en dehors de la période de location, la donnée de localisation du véhicule n'est pas associée à une personne physique identifiée ou identifiable et ne constitue donc pas une donnée personnelle. Par conséquent, le traitement de cette donnée n'est pas soumis au RGPD.

[6] Certaines données techniques du véhicule, telles que le VIN, peuvent être considérées comme personnelles pour certaines organisations, et comme non personnelles pour d'autres, selon qu'elles peuvent être liées ou non à une personne physique identifiable. La Cour de justice de l'Union européenne (CJUE) l'a ainsi rappelé dans son arrêt du 9 novembre 2023 (C-319/22), au point 49.

[7] Sous les conditions prévues à ces articles 2 (champ d'application matériel) et 3 (champ d'application territorial).

Applicabilité de la directive 2002/58/CE du 12 juillet 2002 dite « vie privée et communications électroniques »

Comment savoir si la directive ePrivacy est applicable ?

17. Conformément à l'article 5.3 de la directive 2002/58/CE du 12 juillet 2002 dite « vie privée et communications électroniques » (« directive ePrivacy »), le stockage d'informations ou l'obtention d'un accès à des informations stockées dans l'équipement terminal d'un abonné ou d'un utilisateur n'est autorisé que sur la base du consentement, sauf exceptions.

18. Cette exigence a été **transposée, en droit français, à l'article 82 de la loi Informatique et Libertés**.

19. Cette disposition, interprétée à la lumière de la directive ePrivacy[8], est applicable dès lors que :

- les opérations effectuées **portent sur des « informations »** (qui peuvent être, mais pas exclusivement, des données personnelles) ;
- les opérations effectuées **concernent un « équipement terminal »**[9] **d'un abonné ou d'un utilisateur** qui, pour être qualifié de la sorte, doit avoir la capacité à se connecter à un réseau public de communications [10] ; et
- les opérations effectuées constituent effectivement **un « stockage » ou un « accès ».**

20. Pour rappel, les données de localisation constituent des informations relatives à la localisation d'un objet ou d'une personne. Le véhicule connecté, y compris les appareils qui peuvent lui être raccordés, est généralement considéré comme un « équipement terminal » au même titre qu'un ordinateur, un téléphone mobile multifonction ou une télévision connectée.

21. Par conséquent, **l'article 82 a vocation à s'appliquer en cas d'accès aux données de localisation du véhicule connecté** (produites par son capteur GPS, par exemple).

Quelles conséquences ?

22. **Les utilisateurs doivent être informés et donner leur consentement**[11] **préalablement** à ces opérations, sauf si elles sont strictement nécessaires à la fourniture d'un service expressément demandé par l'utilisateur ou ont pour finalité exclusive de permettre ou faciliter une communication par voie électronique.

23. Le traitement de données personnelles mis en œuvre à partir des données récupérées via ces opérations (aussi appelés les « traitements subséquents ») doit, par ailleurs, reposer sur une des bases légales prévues par l'article 6 du RGPD afin d'être licite[12].

---

[8] Notamment au regard des lignes directrices 2/2023 sur le champ d'application technique de l'article 5(3) de la directive ePrivacy,, CEPD, URL : https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22023-technical-scope-art-53-eprivacy-directive_fr.

[9] La directive 2008/63/Ce de la Commission du 20 juin 2008 relative à la concurrence dans les marchés des équipements terminaux de télécommunications définit la notion de terminal à son article 1er : « *tout équipement qui est connecté directement ou indirectement à l'interface d'un réseau public de télécommunications pour transmettre, traiter ou recevoir des informations; dans les deux cas, direct ou indirect, la connexion peut être établie par fil, fibre optique ou voie électromagnétique; une connexion est indirecte si un appareil est interposé entre l'équipement terminal et l'interface du réseau public* ». Voir également les lignes directrices 2/2023 sur le champ d'application technique de l'article 5(3) de la directive ePrivacy (paragraphes 13 et suivants), CEPD, URL : https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22023-technical-scope-art-53-eprivacy-directive_fr.

[10] Il convient de noter que le fait que le réseau soit mis à la disposition d'un sous-ensemble limité du public (par exemple, des abonnés, payants ou non, soumis à des conditions d'éligibilité) ne fait pas de ce réseau un réseau privé (lignes directrices 2/2023 sur le champ d'application technique de l'article 5(3) de la directive ePrivacy (paragraphe 26), CEPD, URL : https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22023-technical-scope-art-53-eprivacy-directive_fr).

[11] La notion de consentement utilisée dans la directive ePrivacy est identique à celle figurant dans le RGPD : elle doit donc satisfaire à toutes les exigences du consentement prévues à l'article 4, paragraphe 11, et à l'article 7 du RGPD (lignes directrices 01/2020 sur le traitement des données à caractère personnel dans le contexte des véhicules connectés et des applications liées à la mobilité (voir en ce sens le point 16), CEPD, URL : https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-012020-processing-personal-data-context_fr).

[12] Voir le contenu « Les bases légales », CNIL, URL : https://www.cnil.fr/fr/les-bases-legales.

Exemple

Le consentement du locataire d'un véhicule est requis pour le traitement des données personnelles de localisation de ce véhicule à des fins d'amélioration ou d'optimisation du service de location.

Voir les recommandations spécifiques à cette finalité au point 5.3.

24. Par ailleurs, lorsque les données sont collectées sur la base du consentement prévu à l'article 82 de la loi Informatique et Libertés pour une finalité spécifique, elles ne peuvent faire l'objet d'un autre traitement qu'à condition que l'utilisateur ait consenti à cette nouvelle finalité ou que le traitement ait été autorisé par un texte afin de garantir les objectifs prévus à l'article 23.1 du RGPD.

3.2 Poursuivre une finalité déterminée, explicite et légitime

25. La finalité du traitement est l'objectif poursuivi par l'utilisation des données personnelles. Cet objectif doit être **déterminé** (c'est-à-dire établi dès la définition du projet), **explicite** (c'est-à-dire connu et compréhensible) et **légitime** (c'est-à-dire compatible avec les missions de l'organisme).

26. Les données ne doivent pas être traitées ultérieurement de façon incompatible avec cet objectif initial : le principe de finalité limite la manière dont le responsable du traitement peut utiliser ou réutiliser ces données dans le futur.

3.3 Déterminer les rôles de chaque acteur

27. Conformément au principe de responsabilité prévu par le RGPD, **chaque acteur doit déterminer sa qualification au regard de son rôle effectif pour chaque traitement de données personnelles.** Il doit être en mesure d'expliquer la qualification retenue, en précisant les raisons l'ayant conduit à ce choix.

28. Pour ce faire, il est utile de se poser les questions suivantes : qui a décidé de créer le traitement ? Qui a défini sa finalité ? Qui détermine les données personnelles collectées, leurs durées de conservation, les mesures de sécurité mises en place ?

29. Les acteurs doivent être en mesure de démontrer qu'une telle réflexion a été menée. Elle doit être formalisée dans l'analyse d'impact relative à la protection des données lorsque celle-ci est effectuée.

Point d'attention

La qualification des acteurs doit être effectuée au cas par cas. Les exemples ci-dessous ne préjugent pas des qualifications qui pourraient être retenues en pratique, compte tenu de chaque situation particulière.

Les autorités de contrôle ne sont pas liées par les qualifications choisies par les parties, notamment au sein des contrats ; il leur est possible de retenir une qualification différente en fonction du cas d'espèce.

Responsable du traitement

30. Le responsable du traitement désigne la personne qui détermine les finalités et les moyens du traitement des données de localisation[13].

Exemple

Le gestionnaire de flotte agit comme responsable du traitement lorsqu'il décide de géolocaliser les véhicules loués au cours de leurs trajets afin de pouvoir les retrouver en cas de vol et qu'il détermine les moyens d'y parvenir (par exemple, à l'aide d'un système de télématique).

Voir les recommandations spécifiques à cette finalité au point 5.4.

[13] Voir l'article 4.7 du RGPD et les lignes directrices 07/2020 du CEPD sur les notions de responsable de traitement et de sous-traitant dans le RGPD, CEPD, URL : https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-072020-concepts-controller-and-processor-gdpr_fr.

31. Deux ou plusieurs responsables peuvent déterminer conjointement les finalités et les moyens du traitement et peuvent donc être considérés comme des responsables conjoints de celui-ci (article 26 du RGPD). Dans ce cas, ils doivent déterminer clairement leurs obligations respectives, notamment en ce qui concerne l'exercice des droits des personnes concernées et la fourniture des informations visées aux articles 13 et 14 du RGPD.

Exemple

Une autorité organisatrice de la mobilité peut avoir recours à une société privée pour organiser un service de location de véhicules électriques à des tarifs préférentiels afin de favoriser les mobilités douces sur son territoire. L'autorité et la société peuvent être considérées comme responsables conjoints des traitements de données de localisation de ces véhicules lorsqu'elles décident ensemble de les collecter à des fins de lutte contre le vol et s'accordent sur les moyens du traitement de données (fréquence de collecte des données, nombre de positions conservées et durée de conservation de chaque position, organisation de la base de données, mesures de sécurités, etc.).

Sous-traitants

32. Le sous-traitant (au sens du RGPD) désigne toute personne chargée de traiter des données à caractère personnel pour le compte, sur instruction et sous l'autorité du responsable du traitement[14].

Exemple

Un gestionnaire de flotte collecte les données de localisation des véhicules qu'il loue afin d'être en mesure, en cas de suspicion ou de déclaration de vol, de retrouver le véhicule.

Lorsque ce gestionnaire de flotte recourt à un prestataire lui fournissant une plateforme de lutte contre le vol des véhicules reposant sur le traitement de leurs données de localisation, ce prestataire peut être amené à traiter les données de localisation en tant que sous-traitant (par exemple, l'hébergement des données, la transmission des données en cas de vol, etc.).

Dans certaines hypothèses, le gestionnaire de flotte récupère directement les données du véhicule connectées pour obtenir sa localisation, notamment à des fins de lutte contre le vol. Ces données, collectées par le constructeur du véhicule, peuvent lui être mises à disposition par le biais d'une API : dans ce cas, le constructeur et le gestionnaire de flotte sont des responsables de traitement distincts et traitent les données de localisation pour des finalités qui leurs sont propres.

33. Dans ce cadre, il ne traite pas les données pour ses propres fins sans préjudice de la possibilité pour le sous-traitant, dans certaines conditions, de traiter les données pour ses propres finalités, telles que l'amélioration ou l'optimisation de ses produits, par exemple.

Point d'attention

Un sous-traitant ne peut réutiliser des données personnelles pour son propre compte que si cette réutilisation est compatible avec le traitement initial et que le responsable du traitement lui en a donné l'autorisation écrite[15].

[14] Voir article 4.8 du RGPD et les lignes directrices 07/2020 du CEPD sur les notions de responsable de traitement et de sous-traitant dans le RGPD.

[15] Voir le contenu « Sous-traitants : la réutilisation de données confiées par un responsable de traitement », CNIL, URL : https://www.cnil.fr/fr/sous-traitants-la-reutilisation-de-donnees-confiees-par-un-responsable-de-traitement.

Exemple

Un fournisseur de boîtiers télématiques peut collecter et traiter des données de localisation pour le compte d'un gestionnaire de flotte à des fins de lutte contre le vol. Il peut, sous réserve que cette réutilisation soit compatible avec la finalité poursuivie par le gestionnaire de flotte et que ce dernier l'y autorise par écrit, traiter les données collectées pour des finalités qui lui sont propres.

Une réutilisation compatible des données serait par exemple le traitement de données anonymisées afin d'améliorer la précision du boîtier ou la performance du service qu'il fournit en lien avec ce boîtier.

En revanche, la réutilisation de données de localisation identifiantes, par exemple pour développer un autre service aux gestionnaires de flotte fondé sur l'analyse des trajets fréquemment effectués par leurs clients, ne semble pas compatible avec la finalité initiale.

34. En cas de recours à un sous-traitant, un contrat doit être conclu avec le responsable du traitement. Ce contrat doit faire mention des obligations qui incombent respectivement à chacune des parties en matière de protection des données (article 28 du RGPD)[16].

35. Le responsable du traitement doit documenter les instructions qu'il adresse au sous-traitant et qui concernent les modalités de traitement des données (article 22.3.a du RGPD).

3.4 Identifier les personnes concernées

36. La personne concernée peut être :

- Le propriétaire du véhicule, identifiable notamment, via le numéro de la plaque d'immatriculation du véhicule ou encore, le VIN ;
- Le locataire du véhicule, identifié dans le contrat de location ;
- L'utilisateur qui s'est identifié dans le système d'info-divertissement ou qui a connecté son téléphone portable à ce dernier.

37. En pratique, une multiplicité de personnes, conducteurs et passagers, peuvent utiliser un même véhicule : ce seront alors également leurs données de déplacement qui seront traitées. Toutefois, **le responsable du traitement** (par exemple, le constructeur ou le loueur du véhicule) **n'est pas tenu d'identifier les personnes avec lesquelles il n'a pas de relations, notamment contractuelles.** L'absence d'obligation d'authentification du conducteur du véhicule constitue d'ailleurs une mesure favorable à la protection de la vie privée des personnes utilisant le véhicule.

38. Par conséquent, en principe, aucun manquement aux obligations du RGPD ne pourra lui être reproché à l'égard des personnes dont il ne peut avoir raisonnablement connaissance qu'elles utilisent le véhicule ou qu'elles sont présentes dans le véhicule au moment de la collecte des données (les passagers) même si les données collectées pourraient leur être rattachées.

Exemple 1

Il ne pourra être reproché à un constructeur de refuser de répondre favorablement à la demande d'exercice de l'un des droits prévus par le RGPD d'une personne qui n'est pas le propriétaire du véhicule.

En revanche, si le véhicule permet la création de profils sur son système d'info-divertissement ou sur une application dédiée et que cette personne s'est identifiée à un profil qu'elle a créé, il pourra être tenu d'accéder à sa demande, dans les conditions prévues par le RGPD.

[16] Le guide du sous-traitant, édité par la CNIL, précise la nature de ces obligations et les clauses qu'il est recommandé d'intégrer dans les contrats. URL : https://www.cnil.fr/fr/reglement-europeen-sur-la-protection-des-donnees-un-guide-pour-accompagner-les-sous-traitants.

Exemple 2

Un gestionnaire de flotte n'est pas tenu de répondre favorablement à la demande d'exercice de l'un des droits prévus par le RGPD d'une personne qui indique avoir conduit le véhicule loué, dès lors que cette personne n'est pas prévue comme l'un des conducteurs du véhicule dans le contrat de location.

Il en va de même en ce qui concerne les passagers d'un véhicule, pour lesquels le responsable du traitement n'est pas en mesure de savoir si, et quand, ils ont été présents dans le véhicule.

3.5 Identifier les bases légales mobilisables

Une base légale pour chaque finalité

39. Un traitement de données personnelles n'est licite que s'il repose sur l'une des bases légales prévues par l'article 6.1 du RGPD.

40. Lorsqu'un traitement poursuit plusieurs finalités, le responsable du traitement doit déterminer la base légale la plus appropriée pour chacune d'entre elles. Selon l'utilisation prévue des données de localisation, la base légale ne sera donc pas toujours la même.

Point d'attention

Le responsable du traitement doit déterminer ces bases légales pour chaque finalité qu'il poursuit et ce, avant toute opération de traitement, après avoir mené une réflexion, qu'il pourra documenter, au regard de sa situation spécifique et du contexte.

Bases légales mobilisables pour les traitements dont la finalité implique le traitement de données de localisation

Le consentement (article 6.1.a du RGPD)

41. Pour être valable, ce consentement doit être libre, spécifique, éclairé et univoque. A ce titre, et conformément aux articles 4.11 et 7 du RGPD :

- Le consentement doit être recueilli de manière distincte des conditions générales de vente ou d'utilisation, par exemple, sur l'écran d'info-divertissement (article 7.2 du RGPD).
- Il doit être exprimé par une action positive (par exemple, par une case à cocher, non pré-cochée par défaut).
- Le refus de consentir doit être aussi facile à exprimer que le consentement, afin de garantir que ce dernier soit libre.
- La personne concernée doit être en mesure de retirer, à tout moment, son consentement (article 7.3 du RGPD) aussi facilement qu'elle l'a donné.

Point d'attention

Lorsqu'un consentement, au sens de l'article 82 de la loi Informatique et Libertés, est nécessaire pour l'accès ou le stockage d'informations sur le terminal de l'utilisateur, **le consentement, au sens de l'article 6.1.a du RGPD, constitue généralement la base juridique la plus appropriée pour fonder les traitements de données à caractère personnel issues du véhicule connecté**[17].

Lorsque l'accès ou le stockage d'informations sur le terminal de l'utilisateur et le traitement de ces informations poursuivent la même finalité, le consentement requis en vertu de l'article 82 de la loi Informatique et Libertés et le consentement nécessaire comme base juridique pour le traitement de données peuvent être obtenus simultanément, via la même action (par exemple, par le biais d'une case à cocher décochée par défaut).

Le contrat (article 6.1.b du RGPD)

42. Le traitement des données de localisation peut être nécessaire à l'exécution d'un contrat auquel la personne concernée est partie, ou de mesures précontractuelles prises à sa demande.

43. La mobilisation de cette base légale implique de démontrer :

- l'existence d'un contrat valide, auquel la personne concernée par le traitement est partie ; et
- que le traitement est nécessaire au regard de l'objectif du contrat et des attentes mutuelles des parties quant à cet objectif.

44. À cet égard, le responsable du traitement doit être en mesure de démontrer que le traitement est objectivement indispensable pour réaliser une finalité faisant partie intégrante de la prestation contractuelle destinée à la personne concernée. Il doit ainsi prouver que l'objet principal du contrat ne pourrait être atteint en l'absence du traitement en cause.

45. Le fait que le traitement soit mentionné dans le contrat ou qu'il soit seulement utile à l'exécution de celui-ci ne suffit pas à démontrer la nécessité du traitement. Il ne doit donc pas exister d'autres solutions praticables et moins intrusives.

Exemple 1

Le traitement des données de localisation afin de vérifier le kilométrage du véhicule loué, lorsque le contrat de location prévoit un nombre de kilomètres maximal pouvant être parcourus, peut reposer sur la base légale du contrat :

- lorsque le véhicule n'est pas équipé d'odomètre, ou
- à des fins de contrôle de l'exactitude des données de l'odomètre, afin de comparer ces données à la distance calculée à partir des données de localisation et vérifier ainsi leur cohérence (notamment pour identifier les cas de défaut, ou de manipulation de l'odomètre).

En effet, dans ces hypothèses la vérification du nombre de kilomètres effectivement parcouru avec le véhicule est nécessaire pour facturer le service, dès lors que la limitation du nombre de kilomètres est au cœur de la prestation offerte par le contrat, et il n'existe pas de moyens moins intrusifs de calculer le kilométrage.

Voir les recommandations spécifiques à cette finalité au point 5.4.

[17] Lignes directrices 01/2020 sur le traitement des données à caractère personnel dans le contexte des véhicules connectés et des applications liées à la mobilité (voir en ce sens le point 15), CEPD, URL : https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-012020-processing-personal-data-context_fr.

Exemple 2

Le traitement des données de localisation à des fins de lutte contre le vol peut reposer sur la base légale du contrat lorsqu'un particulier a souscrit à un contrat ou une clause contractuelle optionnelle spécifique à cette fin, tel un contrat de pistage ou « *tracking* », reposant sur une solution de localisation embarquée, lui permettant de retrouver son véhicule en cas de vol. En revanche, un tel traitement ne saurait reposer sur un contrat de vente ou de location du véhicule dès lors qu'il n'est pas objectivement nécessaire à la fourniture du bien ou du service. Pour la location, ce traitement peut reposer, à certaines conditions sur la base légale de l'intérêt légitime.

Voir les recommandations spécifiques à cette finalité au point 5.1.

La poursuite d'un intérêt légitime (article 6.1.f du RGPD)

46. L'intérêt légitime poursuivi du responsable du traitement ou du tiers peut être retenu sous réserve du respect des conditions suivantes :

- la légitimité de l'intérêt poursuivi par le responsable de traitement ou le tiers ;
- la nécessité du traitement de données pour poursuivre cet intérêt ; et
- l'absence d'atteinte disproportionnée aux intérêts et droits des personnes concernées, compte tenu des attentes raisonnables des personnes concernées à l'égard de ce traitement[18].

Exemple 1

La collecte de données de localisation par une société de location de véhicule uniquement afin d'être en mesure d'aider un client qui cherche à contester une infraction au code de la route ne peut pas reposer sur la base légale de l'intérêt légitime.

En effet, la société de location n'a pas d'intérêt réel à permettre à ses clients de contester les infractions au code de la route. Même si la société démontrait un tel intérêt, celui-ci resterait purement hypothétique dans la mesure où les données de localisation ne seraient utiles que dans l'hypothèse où l'un des clients aurait commis une infraction lors de la location et ne seraient pertinentes que pour certains types d'infractions.

Exemple 2

La collecte de données de localisation par une société d'assurance de véhicules, avec laquelle aurait contracté une société de location, ou par une société de location de véhicule à des fins générales de « lutte contre la fraude » à l'assurance ne semble pas pouvoir reposer sur la base légale de l'intérêt légitime dès lors que :

- même si un tel intérêt peut être considéré comme légitime, la collecte des données de localisation ne semble pas adéquate pour identifier la majorité des hypothèses de fraude (connaitre la localisation du véhicule ne semble pertinent, pour identifier une fraude, que dans l'hypothèse d'une déclaration qui indiquerait qu'un accident se serait produit à un autre lieu que le lieu réel de l'accident ; cette donnée ne semble pas pertinente, par exemple pour les cas d'accidents où l'assuré aurait organisé un faux accident). En outre, des moyens moins intrusifs semblent pouvoir être utilisés dans la majorité des hypothèses (tels que le recours à un expert pour identifier la cause de l'accident) ;
- enfin, la collecte et les conservations des données de localisation de l'ensemble des véhicules, tout au long de leur parcours, est disproportionné au regard de l'intérêt à lutter contre la fraude, notamment eu égard au nombre de cas de fraude à l'assurance pour lesquels le recours aux données de géolocalisation serait pertinent.

[18] Ces conditions sont prévues par l'article 6.1.f et le considérant 47 du RGPD, régulièrement rappelées par la jurisprudence de la Cour de justice de l'union européenne (voir notamment CJUE, 4 mai 2017, Rīgas satiksme, C-13/16, point 28) et sont développées dans les lignes directrices 1/2024 sur les traitements basés sur l'article 6(1)(f) du RGPD (soumises à consultation publique et disponibles, uniquement en anglais à ce stade, accessibles sous ce lien : https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2024/guidelines-12024-processing-personal-data-based_en).

L'exécution d'une mission d'intérêt public (article 6.1.e du RGPD)

47. La possibilité de se fonder sur la base légale de la « mission d'intérêt public » suppose :

- que la mission dans laquelle s'inscrit le traitement soit prévue par un texte applicable au responsable du traitement
- que l'utilisation des données permette d'exercer spécifiquement cette mission de manière pertinente et appropriée.

Exemple

Le code des transports donne compétence à l'établissement public Île-de-France mobilités (IDFM) pour organiser des services relatifs aux mobilités actives ou contribuer au développement de ces mobilités, et notamment pour organiser un service public de location de vélos[19].

Ce texte confie ainsi à IDFM une mission d'intérêt public relative à l'organisation d'un service public de location de vélos.

Par conséquent, IDFM peut fonder les traitements de données personnelles qui lui permettent d'exercer cette mission sur cette base légale. Notamment, la collecte et le traitement des données de localisation des vélos peut être nécessaire pour vérifier les usages non conformes au règlement de ce service (comme, par exemple, le fait d'utiliser les vélos proposés en location dans une autre région que l'Île-de-France alors que le service est réservé aux franciliens).

L'obligation légale (article 6.1.c du RGPD)

48. Le traitement des données de localisation peut être fondé sur le respect d'une obligation légale, prévue par un texte (de droit français ou européen) qui s'impose au responsable du traitement, sous réserve que :

- l'obligation soit impérative, suffisamment claire et précise ;
- le(s) texte(s) créant cette obligation définissent au moins la finalité du traitement ; et que
- cette obligation s'impose au responsable du traitement et non aux personnes concernées par le traitement.

49. Le traitement doit être nécessaire pour répondre à cette obligation : il ne doit pas exister de moyen moins intrusif d'atteindre cet objectif que de mettre en œuvre le traitement envisagé.

Exemple

Depuis 2018, plusieurs types de véhicules doivent être obligatoirement équipés d'un système embarqué, dénommé « eCall », qui permet de déclencher automatiquement un appel vers le 112, numéro d'appel d'urgence européen, en cas d'accident grave sur le territoire de l'Union européenne afin d'envoyer rapidement les services de secours sur les lieux.

Le règlement (UE) 2015/758 du 29 avril 2015 prévoit le traitement de certaines données personnelles par le système eCall, telles que les trois dernières positions connues du véhicule (latitude et longitude). Le traitement de ces données de localisation repose donc sur cette obligation légale.

[19] Cette mission, confiée à IDFM, est prévue par le 4° du I de l'article L1241-1 du code des transports (accessible sous ce lien : https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000039787268).

3.6 Appliquer les principes de minimisation et de limitation de la conservation des données de localisation

La minimisation des données collectées

50. Les données personnelles qui font l'objet d'un traitement doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités poursuivies (article 5.1.c du RGPD).

51. En ce qui concerne les traitements de données de localisation des véhicules, il est généralement suffisant que chaque donnée de localisation collectée soit remplacée par la suivante de sorte que seule la dernière position du véhicule soit conservée. Si la dernière position n'est pas suffisante pour poursuivre l'objectif, le responsable du traitement devra être en mesure de justifier de la nécessité de conserver d'autres points de localisation au regard des finalités poursuivies.

52. En tout état de cause, le responsable du traitement doit être en mesure de **justifier la fréquence de la collecte, ainsi que la nature et le volume de données remontées sur ses serveurs,** au regard de chacune des finalités poursuivies.

Exemple 1

La conservation par un gestionnaire de flotte de l'intégralité des données de localisation de chaque véhicule, à une fréquence rapprochée (par exemple, tous les 500 mètres), et pour chaque contrat de location, n'est pas justifiée au regard des finalités de gestion de la flotte de véhicules et du service, de prévention et de lutte contre le vol ainsi que d'assistance à l'utilisateur en cas d'accident[20].

Exemple 2

La conservation, par un fournisseur de services privés d'assistance en cas d'accident, des trois dernières positions du véhicule est, en principe, justifiée pour la finalité d'assistance poursuivie. Les trois dernières positions sont en effet nécessaires, et suffisantes, pour le fonctionnement du système afin de permettre aux secours d'identifier précisément la position du véhicule et le sens de circulation sur la voie sur laquelle il se trouve.

53. La CNIL recommande aux acteurs de privilégier les traitements de données de localisation en local, au sein du véhicule ou du dispositif connecté au véhicule, lorsque cela est possible au regard des finalités poursuivies. Dans ce cas, le traitement est effectué uniquement en local, au sein du véhicule ou du dispositif dont il est équipé, de sorte que les données de localisation sont remontées sur les serveurs du responsable du traitement qu'après un fait générateur (par exemple, une déclaration de panne du véhicule) ou que seuls d'autres types de données soient remontés (par exemple, une alerte correspondant à l'entrée du véhicule dans une zone prohibée ; le nombre de kilomètres parcourus par le véhicule et calculé à partir de la données de localisation ; des données de localisation agrégées, etc.).

54. Dans d'autres cas, il sera nécessaire de remonter les données de localisation en continu au sein des serveurs du responsable du traitement **(voir l'encadré, « Cas d'une base de données servant des finalités multiples »).**

Cas d'une base de données servant des finalités multiples

Lorsqu'un organisme choisit de recourir à une base de données de géolocalisation unique permettant de servir la **réalisation de plusieurs traitements aux finalités distinctes, les principes de minimisation et de limitation de la durée de conservation s'appliquent à chacun des traitements.** Il n'est pas pour autant nécessaire de constituer autant de base de données qu'il y a de traitement.

Ainsi, la CNIL recommande que la minimisation soit mise en œuvre via des mesures techniques qui évitent d'enregistrer « par excès » des séries de données à la fois très fréquentes et très précises dont une partie ne seraient nécessaires à la réalisation d'aucune des finalités poursuivies. De même, la CNIL recommande que la

[20] Voir la décision du Conseil d'État, 6 décembre 2023, n°467368 (accessible sous ce lien : https://www.legifrance.gouv.fr/ceta/id/CETATEXT000048527626)

limitation de la durée de conservation soit mise en œuvre à travers des règles techniques qui assurent qu'aucune ligne de la base n'est conservée si elle n'est plus nécessaire pour la réalisation d'aucune des finalités prévues.

N. B. : les recommandations techniques applicables au cas de la base de données servant plusieurs finalités sont présentées en partie 3.6.

55. Il appartient aux responsables du traitement de démontrer, au cas par cas, la nécessité de collecter les données de localisation ainsi que celle de les remonter sur des serveurs distants.

La durée de conservation des données

56. Conformément à l'article 5.1.e du RGPD, les données personnelles ne doivent être conservées sous une forme permettant l'identification des personnes que le temps strictement nécessaire à la réalisation des finalités poursuivies. C'est donc au regard de la finalité que la durée de conservation doit être déterminée par le responsable du traitement, en amont de la mise en œuvre du traitement.

57. Les données peuvent être conservées sous forme d'archives intermédiaires, distinctes de la base active, avec accès restreint, conformément aux dispositions législatives ou réglementaires spécifiques applicables, par exemple, pour répondre à des obligations comptables, sociales ou fiscales ou lorsque ces données présentent un intérêt en cas de contentieux, justifiant de les conserver le temps des règles de prescription applicables.

Exemple 1

Dans le cadre de la location d'un véhicule, la localisation peut être collectée à des fins de lutte contre le vol : la conservation de la dernière position du véhicule, chaque nouvelle position écrasant la précédente, semble suffisante en l'absence d'évènement permettant de suspecter un vol. En cas de vol (qui aurait, par exemple, été signalé au gestionnaire de flotte), il peut être nécessaire de conserver plus de données que la seule dernière position. Il reviendra au responsable du traitement d'être en mesure de démontrer la nécessité de conserver ces données. Elles ne pourront, en tout état de cause, être conservées que pour une durée maximale de six ans, conformément à la prescription légale applicable.

Voir les recommandations spécifiques à cette finalité au point 5.1.

Exemple 2

Les données de localisation d'un véhicule loué, collectées à des fins d'optimisation du service[21], ne peuvent être conservées sous une forme identifiante que le temps nécessaire à leur anonymisation, lorsque des données anonymisées sont suffisantes pour atteindre cette finalité.

Voir les recommandations spécifiques à cette finalité au point 5.3.

Point d'attention

La CNIL rappelle que sont des **tiers autorisés** les officiers de police judiciaire, de la police et de la gendarmerie lorsqu'ils demandent à se faire communiquer des données personnelles dans le cadre d'une enquête préliminaire, d'une enquête de flagrance ou d'une commission rogatoire, dans les conditions prévues par le code de procédure pénale. En cas de réquisition judiciaire et dès lors qu'elles sont disponibles, les données de localisation doivent être transmises aux autorités judiciaires compétentes par les acteurs concernés (par exemple, le constructeur d'un véhicule). Dans de telles circonstances, la règlementation relative à la protection des données personnelles constitue pas un obstacle, par principe, à cette transmission.

[21] Par exemple, l'optimisation et l'amélioration des fonctionnalités du véhicule et de ses équipements, la maintenance prédictive ou encore l'amélioration des services connectés ou des services du gestionnaire de flottes.

3.7 Assurer l'information des personnes concernées et la mise en œuvre de leurs droits

L'information des personnes concernées

Lorsque les données sont collectées directement auprès des personnes concernées

58. Les personnes concernées doivent être informées, au moment de la collecte de leurs données, de **l'existence du traitement**, de **ses caractéristiques** et **des droits** dont elles disposent en vertu du RGPD. Cette information doit contenir l'ensemble des mentions prévues par l'article 13 du RGPD.

59. Les personnes concernées peuvent, par exemple, être informées **au moyen de clauses concises et aisément compréhensibles figurant dans le contrat** de vente ou de location du véhicule ou encore dans le contrat de prestation de services et/ou tout support écrit, de documents distincts (par exemple, le carnet d'entretien ou le manuel du véhicule) ou de l'écran d'info-divertissement.

60. Cette information doit être clairement distinguée des autres clauses du contrat (de vente ou de location du véhicule) ou d'informations qui ne sont pas liées à la protection des données personnelles.

Lorsque les données ne sont pas collectées directement auprès des personnes concernées

61. Le responsable du traitement des données doit indiquer, en plus des informations prévues à l'article 13 du RGPD, les catégories de données personnelles concernées et la source dont proviennent ces données.

62. Le responsable du traitement doit fournir ces informations dans un délai raisonnable après l'obtention des données, et **au plus tard à la première des dates suivantes**, conformément à l'article 14 du RGPD :

- **un mois après l'obtention des données**, eu égard aux circonstances particulières dans lesquelles les données à caractère personnel sont traitées ; ou
- **lors de la première communication** avec la personne concernée, ou
- si ces données sont communiquées à un tiers, **avant leur transmission**.

Exemple 1

Lorsqu'une personne souscrit à un contrat de location de véhicule, et que des données de localisation seront collectées au cours de la location pour différentes finalités (lutte contre le vol, gestion commerciale de flotte, etc.), elle doit être informée des traitements de données personnelles au moment de la signature du contrat. Cette information peut être dispensée de différentes manières (fourniture de la politique de confidentialité, avec une case à cocher « *j'ai pris connaissance de la politique de confidentialité* », à la première utilisation de l'application de location dédiée ; via la fourniture d'un formulaire papier explicitant les traitements de données personnelles à la personne dans l'agence de location de véhicule, etc.).

Exemple 2

Lorsqu'une personne utilise un véhicule connecté, qu'elle a loué, il est possible que les données de localisation soient collectées par le constructeur pour certaines finalités. Certains constructeurs mettent à disposition des loueurs de véhicules les données du véhicule connecté, soit directement par le biais d'une API, soit par l'intermédiaire d'un agrégateur de données. Dans ces hypothèses, le loueur ne collecte pas les données directement auprès des personnes concernées.

Le loueur doit donc informer ses clients de la collecte indirecte de leurs données personnelles (par exemple, au moment de la signature du contrat de location), en précisant les catégories de données personnelles concernées (notamment les données de localisation) et la source dont proviennent ces données (le constructeur automobile).

63. La CNIL recommande que l'information soit fournie **par différents niveaux notamment dans l'environnement numérique** (liens cliquables, menus dépliants, etc.) afin que les personnes puissent naviguer aisément dans le ou les différents documents et trouver rapidement l'information recherchée. Cela permet également d'apporter des informations plus détaillées, voire descriptives sur le plan technique, sans nuire à l'ergonomie et à la lisibilité de l'information. Une bonne pratique peut être de **recourir, en complément, à des outils pour assurer la transparence de l'information, comme des icônes ou des vidéos.**

64. **L'information doit être délivrée de manière concise, transparente, compréhensible et aisément accessible**, en des termes clairs et simples (article 12.1 du RGPD). Lorsqu'elle implique de recourir à des termes techniques, il est recommandé de fournir une définition ces termes.

Une bonne pratique est de recourir à différents modes d'informations, complémentaires, afin d'assurer la bonne information de l'utilisateur du véhicule mais aussi des autres utilisateurs et passagers :

- mettre à disposition une politique de confidentialité au sein du véhicule (au format papier et/ou par le biais de l'écran d'info-divertissement du véhicule, selon les possibilités offertes au responsable du traitement)
- informer l'utilisateur sur les traitements de localisations lorsqu'il active, pour la première fois, une fonctionnalité qui implique de tels traitements ;
- utiliser une icône (qui peut notamment figurer sur l'écran d'info-divertissement du véhicule) lorsque les données de localisation du véhicule sont collectées ;
- recourir à des représentations graphiques, telles que des schémas explicitant les données colletés et les flux associés (données traitées uniquement en local, données remontées sur des serveurs externes au véhicule, etc.), soit dans la politique de confidentialité, soit sur le site internet du responsable du traitement ;
- apposer un sticker, pouvant comprendre un QR code, sur le véhicule pour signaler qu'il est connecté et rediriger vers la politique de confidentialité (notamment afin que l'ensemble des utilisateurs potentiels puissent s'informer des traitements de données mis en œuvre), etc.

Le recours à ces différents modes d'information de manière combinée peut être pertinent pour garantir la bonne information des utilisateurs du véhicule connecté (notamment dans la mesure où certains utilisateurs peuvent ne pas disposer d'un appareil ou des connaissances nécessaires pour accéder aux informations si elles sont uniquement fournies par un QR code, par exemple).

Par ailleurs, bien que chaque responsable du traitement soit tenu d'assurer l'information des personnes concernées sur les traitements qu'il met en œuvre, il semble pertinent de faciliter l'accès à cette information. De même, constitue une bonne pratique la mise à disposition d'un tableau récapitulant, par marque de véhicule proposé à la location, les coordonnées du délégué à la protection des données de chaque constructeur, afin de faciliter la mise en œuvre des droits des personnes concernées auprès de ces derniers.

Exemple

Les gestionnaires de flotte de véhicules loués peuvent mettre à disposition de leurs clients une fiche explicative des traitements opérés par chaque constructeur, renvoyant vers leur politique de confidentialité (adaptée pour chaque modèle de véhicule loué) et indiquant les coordonnées du délégué à la protection des données ou de la personne à contacter chez le constructeur pour exercer ses droits.

L'exercice des droits des personnes concernées

65. L'exercice par les personnes concernées des différents droits prévus aux articles 15 à 22 du RGPD doit être garanti.

Les responsables des traitements doivent notamment veiller à ce que les personnes concernées puissent facilement exercer leurs droits (accès, rectification, effacement, limitation du traitement et, en fonction de la base juridique du traitement, droit à la portabilité des données et droit d'opposition).

66. À cet égard, des outils spécifiques peuvent être mis en œuvre afin de permettre aux personnes concernées d'exercer efficacement leurs droits[22] :

[22] Conformément aux recommandations du CEPD (Lignes directrices 01/2020 sur le traitement des données à caractère personnel dans le contexte des véhicules connectés et des applications liées à la mobilité, voir en ce sens les points 90 et suivants, accessibles sous ce lien : https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-012020-processing-personal-data-context_fr).

- Ainsi, pour faciliter la modification des paramètres, il peut être pertinent de mettre en place un système de gestion des profils pour conserver les préférences des conducteurs connus et les aider à modifier facilement et à tout moment leurs paramètres de confidentialité.
- D'une manière générale, la CNIL recommande de centraliser à un seul et même endroit (dans le véhicule et éventuellement dans l'application dédiée) tous les paramètres de données pour chaque traitement, notamment pour faciliter l'accès, l'effacement, la suppression et la portabilité des données à caractère personnel des systèmes du véhicule à la demande de la personne concernée.

67. En outre, afin de permettre aux personnes concernées de supprimer rapidement et facilement les données personnelles susceptibles d'être conservées, il est recommandé aux constructeurs de prévoir une fonction simple (comme un bouton de suppression au sein du véhicule ou dans l'application utilisée en lien avec le véhicule). L'effacement des données personnelles est en effet particulièrement important en cas de location du véhicule ou en cas de cession du véhicule, afin que le locataire ou le propriétaire suivant n'ait pas accès aux données de déplacement du précédent.

68. Par ailleurs, le recours à des modalités pratiques permettant d'améliorer la bonne compréhension des traitements par les personnes concernées constitue une bonne pratique (par exemple en fournissant une représentation graphique, en réponse à une demande de droit d'accès afin d'illustrer les données de localisation que conserve le responsable du traitement).

3.8 Adopter des mesures de sécurité pour encadrer les traitements de données de localisation

69. Les mesures de sécurité encadrant les traitements de données de localisation sont essentielles au regard des risques pour la vie privée. Afin de garantir la confidentialité, l'intégrité et la disponibilité de ces données, la CNIL recommande de mettre en place des mesures techniques et organisationnelles robustes, dont les principales sont développées ci-après.

Gestion des risques relatifs à la cybersécurité

70. L'écosystème des véhicules connectés dispose d'un ensemble de normes techniques d'application obligatoire ou volontaire permettant aux responsables de traitement de mettre en place une gestion des risques liés à la cybersécurité.

71. Parmi ces normes techniques, le règlement ONU n°155[23] se concentre par exemple sur l'homologation de la cybersécurité des véhicules et de leurs systèmes de gestion. D'autres règlements ONU existent concernant des problématiques plus spécifiques, tels que les systèmes de mise à jour à distance des véhicules (règlement ONU n° 156[24]) et les systèmes automatisés de maintien de la trajectoire (règlement ONU n° 157[25]).

72. La norme internationale ISO/SAE 21434[26] spécifie les exigences techniques pour la gestion du risque de cybersécurité en ce qui concerne la conception, le développement de produits, la production, l'exploitation, la maintenance et la mise hors service des systèmes électriques et électroniques dans les véhicules routiers, y compris leurs composants et interfaces.

73. La norme ISO/SAE 21434 est une norme volontaire, ce qui signifie qu'elle n'est pas obligatoire pour les fabricants de véhicules et les autres parties prenantes. En revanche, les règlements ONU 155, 156 et 157 sont des règlements obligatoires qui doivent être respectés par les fabricants de véhicules et les autres parties prenantes dans les pays qui ont adopté ces règlements.

---

[23] Règlement ONU no 155 — Prescriptions uniformes relatives à l'homologation des véhicules en ce qui concerne la cybersécurité et de leurs systèmes de gestion de la cybersécurité [2021/387] (OJ L 82 09.03.2021, p. 30, ELI: http://data.europa.eu/eli/reg/2021/387/oj)

[24] Règlement ONU no 156 — Prescriptions uniformes relatives à l'homologation des véhicules en ce qui concerne les mises à jour logicielles et le système de gestion des mises à jour logicielles [2021/388] (OJ L 82 09.03.2021, p. 60, ELI: http://data.europa.eu/eli/reg/2021/388/oj)

[25] Règlement ONU no 157 — Prescriptions uniformes relatives à l'homologation des véhicules en ce qui concerne leur système automatisé de maintien dans la voie [2021/389] (OJ L 82 09.03.2021, p. 75, ELI: http://data.europa.eu/eli/reg/2021/389/oj)

[26] Norme internationale ISO/SAE 21434:2021 Véhicules routiers — Ingénierie de la cybersécurité (disponible en anglais sous ce lien : https://www.iso.org/obp/ui/en/#iso:std:iso-sae:21434:ed-1:v1:en), iso.org

74. L'application de normes volontaires telles que l'ISO/SAE 21434 est fortement recommandée par la CNIL : ce type de normes implique l'engagement de la direction générale pour le développement de produits et normalise les rôles et responsabilités dans les chaînes d'approvisionnement. Elle permet également de définir les phases du cycle de vie du produit avec des objectifs précis tout en incluant l'analyse des menaces et l'évaluation des risques de cybersécurité.

Point d'attention

Les recommandations qui vont suivre concernant la sécurité des données de localisation doivent donc être lues à la lumière des normes existantes applicables aux véhicules connectés et leur écosystème. Elles ne visent pas à remplacer ces normes techniques mais à fournir des éclaircissements complémentaires relatifs à la sécurité de ces données ainsi qu'à la conformité à la réglementation relative aux données personnelles. Ces recommandations peuvent également être applicables à des systèmes traitant des données de localisation et n'étant pas inclus dans le périmètre de ces normes.

Chiffrement en transit et au repos

75. Etant donné le caractère très intrusif pour la vie privée et les possibilités d'inférence[27] des données de localisation, la CNIL recommande de chiffrer les données de localisation au repos (données stockées en mémoire secondaire, qui ne sont pas en cours d'utilisation) et en transit (tous les échanges de données via des réseaux de communication) dans et entre les différents systèmes pouvant les collecter ou les traiter. Ces mesures techniques permettent de lutter contre les conséquences du vol des supports de données ou de l'interception des communications.

76. Si cette recommandation vise en particulier les supports amovibles ou mobiles. Elle constitue une bonne pratique pour l'ensemble des supports de stockage susceptibles de contenir des données de géolocalisation.

77. Les algorithmes et protocoles de chiffrement devraient être mises en œuvre selon l'état de l'art, par exemple l'annexe B1 du Référentiel Général de Sécurité[28]. Il est recommandé aux responsables du traitement de choisir des solutions et bibliothèques cryptographiques éprouvées, auditées et maintenues.

Habilitation

78. De manière générale, la CNIL recommande de définir des profils d'habilitation afin de gérer les accès systèmes traitant des données de localisation, dont les permissions sont strictement ajustées aux besoins, d'une durée déterminée et limitée.

79. Les permissions d'accès devraient être retirées dès le retrait des habilitations, par exemple après le départ d'un collaborateur ou une modification de ses missions.

80. Une revue des habilitations devrait être réalisée régulièrement et a minima annuellement.

81. Chaque personne habilitée à accéder à des données de localisation devrait être authentifiée avant d'accéder à ces données personnelles, ainsi qu'aux autres données pouvant y être associées.

Limitation des accès

82. Afin de prévenir les tentatives massives d'accès aux données, la CNIL recommande que des mesures relatives à la limitation des accès aux systèmes traitant des données de géolocalisation soient mises en place.

83. En plus des profils d'habilitation adéquats exposés précédemment, les acteurs devraient s'assurer de l'existence de limitations temporelles sur le nombre de requêtes pouvant être effectuées sur ces systèmes ainsi que sur les volumes de données exportables. Ces paramètres peuvent être limités globalement ou individuellement au niveau des utilisateurs ou administrateurs.

---

[27] Attaque par inférence : l'attaquant prend en entrée un jeu de données de localisation (et éventuellement quelques connaissances préalables) et tente de déduire des informations personnelles concernant les individus contenus dans le jeu de données.

[28] Le référentiel général de sécurité version 2.0 : les documents, cyber.gouv.fr (accessible sous ce lien : https://cyber.gouv.fr/le-referentiel-general-de-securite-version-20-les-documents)

84. Les profils d'habilitation peuvent également être limités non seulement par des rôles spécifiques, mais aussi par des périmètres temporels, par exemple les horaires de travail, et géographiques précis.

85. Enfin, les durées de conservation de ces données devraient être mises en œuvre *via* un mécanisme d'archivage ou de purge automatique.

Authentification

86. Dans la définition de leur politique d'accès et d'authentification, les acteurs sont invités à se référer à la délibération n° 2022-100 du 21 juillet 2022 portant adoption d'une recommandation relative aux mots de passe et autres secrets partagés[29].

87. Dans le cas de l'utilisation de comptes à privilèges, tels que des comptes administrateur, ces comptes devraient être protégés par une authentification renforcée s'appuyant sur des technologies d'authentification multifacteur. Les facteurs d'authentification fondées sur des facteurs de connaissance et de possession sont à privilégier. Les responsables du traitement peuvent se référer aux recommandations de la CNIL sur ce sujet.

88. Dans le cas où des transmissions de données de localisation sont effectuées, ces transmissions ne devraient pas reposer sur des secrets tels que des mots de passe stockées dans le système assurant les transmissions, mais au moins sur une authentification mutuelle des serveurs ainsi qu'avec une authentification par certificats serveur.

Journalisation et analyse des accès et des opérations

89. Les différentes opérations de création, consultation, modification et suppressions relatives à une base de données de localisation doivent être tracées par l'entité responsable de cette base. La CNIL recommande à ce titre que ces opérations fassent l'objet d'un enregistrement comprenant la personne habilitée individuellement identifiée, l'horodatage, la nature de l'opération réalisée ainsi que la référence des données concernées par l'opération. Lorsque les dispositifs, notamment embarqués, ont un espace trop restreint pour journaliser les opérations, ces opérations peuvent être journalisées au sein des serveurs traitant les données en provenance de ces dispositifs.

90. La CNIL recommande (voir délibération n° 2021-122 du 14 octobre 2021 portant adoption d'une recommandation relative à la journalisation[30]) que les traces de journalisation de systèmes traitant des données de localisation soient conservées pendant une durée comprise entre six mois et un an à compter de leur collecte, sauf justification particulière démontrant un risque élevé pour les personnes concernées nécessitant de conserver ces traces au-delà de la durée recommandée.

91. La CNIL recommande une surveillance régulière des traces de journalisation et, quand cette dernière est insuffisante au regard de l'échelle du système, la mise en place d'un contrôle automatique ou semi-automatique des traces de journalisation, afin de détecter d'éventuelles anomalies.

92. Il est rappelé que les traces de journalisation ne devraient pas contenir de données sensibles ou d'informations secrètes.

Sauvegardes et continuité d'activité

93. De manière générale, des sauvegardes complètes ou incrémentales devraient être prévues à intervalles réguliers, y compris pour les systèmes comprenant des données de localisation.

94. Les supports de sauvegardes devraient être conservés dans un lieu sûr et différent des données de production, de préproduction ou de développement.

95. Les sauvegardes des données personnelles devraient faire l'objet d'un chiffrement au repos respectant l'état de l'art, et notamment les indications contenues dans les guides de bonnes pratiques, recommandations nationales ou européennes.

---

[29] Délibération n° 2022-100 du 21 juillet 2022 portant adoption d'une recommandation relative aux mots de passe et autres secrets partagés et abrogeant la délibération n° 2017-012 du 19 janvier 2017, legifrance.fr (accessible sous ce lien : https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000046432885)

[30] Délibération n° 2021-122 du 14 octobre 2021 portant adoption d'une recommandation relative à la journalisation, legifrance.fr (accessible sous ce lien : https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000044272396).

96. Un plan de reprise et de continuité d'activité informatique devrait être prévu. Il devrait s'assurer que les utilisateurs et les sous-traitants ultérieurs savent qui contacter en cas d'incident. Ce plan de continuité ou de reprise d'activité ainsi que la restauration des sauvegardes devraient être régulièrement testés.

Systèmes embarqués

97. Des recommandations spécifiques aux systèmes embarqués peuvent être trouvées dans la fiche « Boitiers télématiques et agrégateurs de données ».

3.9 Appliquer les mesures de protection des données dès la conception

98. Pour les concepteurs de systèmes traitant des données de localisation, il est important d'anticiper les risques potentiels et de mettre en place des mesures préventives pour protéger les données personnelles des utilisateurs. Par exemple, les véhicules connectés doivent être conçus avec des paramètres par défaut qui assurent un niveau de protection adéquat des données de localisation, sans nécessiter d'intervention de la part du conducteur.

99. Outre les recommandations précédentes relatives à la minimisation des données et à leur sécurité, la CNIL recommande de mettre en place les mesures techniques et organisationnelles suivantes dès la conception de ces systèmes.

Mesures applicables à la pseudonymisation des données

100. Lorsque les données de localisation sont destinées à être pseudonymisées, la CNIL recommande que cette opération intervienne le plus tôt possible.

101. Si le numéro VIN est associé aux données de localisation, celui-ci devrait être séparé des données de localisation dès que le traitement de ces données ne nécessite plus l'usage du VIN. Il est notamment possible pseudonymiser le VIN en utilisant des fonctions de hachage à l'état de l'art résistantes aux attaques connues, notamment celles utilisées pour le stockage de secrets tels que les mots de passe (par exemple : la fonction « argon2 »[31] qui comprend l'usage d'un sel et de paramètres relatifs aux coûts en temps et/ou en mémoire nécessaires à une attaque par force brute).

102. La pseudonymisation des informations, notamment administratives, relatives aux conducteurs est de même fortement recommandée le plus tôt possible.

Exemple

La production de statistiques relatives à des trajets est un traitement de données à caractère personnel. Les données en entrée de ce traitement devraient être pseudonymisées en amont car les informations administratives relatives aux conducteurs ne sont pas utiles pour la génération des statistiques.

Généralisation des données dès leur collecte

103. La précision des données de localisation collectées dépend avant tout de la technologie utilisée : de quelques mètres par exemple avec des systèmes de géopositionnement tels que Galileo ou GPS, à quelques centimètres pour des systèmes de positionnement à haute précision.

104. La CNIL recommande de généraliser[32] les données autant que possible dès leur réception en provenance du capteur. Cette généralisation pourra être effectuée de préférence au sein du système embarqué qui a collecté la donnée (par exemple un véhicule ou un boitier), ou dès leur réception par un serveur distant.

105. Il faut également mentionner que plus des données de localisation sont précises et plus celles-ci risquent d'être inexactes : une généralisation des données permet également de diminuer la marge d'erreur lors du traitement de ces données, et ainsi d'augmenter l'exactitude des données.

---

[31] Plus d'informations accessibles sous ce lien : https://fr.wikipedia.org/wiki/Argon2

[32] La généralisation consiste à rendre les données moins précises afin que les valeurs soient communes à plusieurs lignes (ou personnes). Elle peut consister par exemple à remplacer des valeurs exactes par des valeurs arrondies, par des intervalles ou ensemble de valeurs prédéfinis, etc.

Séparation logique des données

106. Les données de localisation, lorsqu'elles sont remontées sur les systèmes du responsable de traitement ou de son sous-traitant, peuvent être « cloisonnées » selon certaines modalités, par exemple afin qu'une atteinte à la confidentialité des données d'une partie du système n'entraîne pas directement la perte de confidentialité de données d'une autre partie de celui-ci. La nécessité de mettre en place un tel « cloisonnement » des données peut notamment apparaître :

- en raison de l'utilisation de données distinctes par des clients différents : pour répondre, notamment, à l'obligation d'assurer la confidentialité des données personnelles ;
- en raison de l'utilisation des mêmes données pour des finalités différentes par un même client : pour répondre, notamment, à l'obligation de minimisation des données traitées.

107. D'un point de vue technique, les modalités techniques pour un tel « cloisonnement » peuvent être de différents niveaux :

- cloisonnement physique, en utilisant des serveurs informatiques ou des hébergeurs différents ;
- cloisonnement réseau, en partitionnant le réseau en sous-réseaux de façon à limiter l'accès entre les sous-réseaux (par exemple avec des VLANs) ;
- cloisonnement cryptographique, par du chiffrement au repos avec des clés de chiffrement distinctes en fonction des données à séparer ;
- séparation logique, par l'usage de bases de données différentes, de permissions, de vues ou de contrôles différenciés en fonction des profils d'habilitation.

108. Dans le contexte des données de localisation issues de véhicules connectés, **la CNIL recommande de mettre en place au moins une séparation logique**, qui peut donc prendre la forme, par exemple, d'une base unique avec des profils d'habilitation et de droits d'accès différenciés en fonction de chaque client et de chaque finalité poursuivie.

109. De manière générale, la CNIL recommande de choisir un mode de « cloisonnement » en fonction des risques associés aux données de localisation. Plus les risques liés à la confidentialité, à l'intégrité et à la disponibilité des données sont importants, plus la modalité de cloisonnement devra, en principe être robuste (le cloisonnement physique et réseau pouvant à cet égard offrir les garanties les plus fortes).

Le cloisonnement par client

110. Lorsque des données de localisation sont stockées par un acteur qui détient des données concernant plusieurs clients professionnels (par exemple, un agrégateur de données proposant ses services à plusieurs loueurs de véhicules), les données de localisation spécifiques à un client devraient être cloisonnées des données des autres clients.

111. Comme indiqué précédemment, les modalités techniques de cloisonnement dépendent des risques mais doivent *a minima* empêcher un client professionnel, ou un attaquant, d'accéder aux données des autres clients.

Le cloisonnement par finalité

112. Lorsque la collecte de données de localisation vise à réaliser plusieurs traitements ultérieurs aux finalités distinctes, il n'est pas toujours possible de minimiser la collecte de données au niveau du capteur. Cette situation peut conduire à la collecte de données très précises et très fréquentes, alors que ce niveau de granularité n'est nécessaire pour aucun des traitements individuels à réaliser. Dans un tel cas, la CNIL recommande, lorsque c'est raisonnablement possible, d'enregistrer les données collectées en base avec un niveau de précision variable au long d'une même série, ajusté en fonction de la nécessité pour les traitements subséquents.

113. De plus, en cas d'utilisation d'une même base de données pour la réalisation de plusieurs traitements aux finalités distinctes, la CNIL recommande de recourir à des mesures de cloisonnement afin de gérer les données le plus fidèlement possible au regard du principe de minimisation. Ces mesures s'accompagneraient alors, pour les accédants à la base de données, d'habilitations et de permissions d'accès aux données adaptées en fonction des finalités qu'ils contribuent à poursuivre.

Exemple

Par exemple, dans le cas où un responsable de traitement doit collecter des données de localisation précises et régulières pour lutter contre le vol mais seulement un point approximatif toutes les deux heures pour s'assurer que le véhicule reste sur un territoire donné, la CNIL recommande de cloisonner les deux traitements, par exemple en créant deux vues minimisées de la même base de données correspondant à chacun des deux usages, assorties d'habilitations distinctes et de mesures de traçabilité. Il serait possible, alternativement, d'atteindre le même objectif en créant deux bases minimisées distinctes pour chacun des deux usages.

3.10 Réaliser une analyse d'impact sur la protection des données

Identifier quand une analyse d'impact est nécessaire

114. Une analyse d'impact sur la protection des données (AIPD) doit être réalisée lorsque le traitement est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes concernées (article 35 du RGPD). Cette démarche permet de cartographier et d'évaluer les risques d'un traitement sur la protection des données personnelles et d'établir un plan d'action pour les réduire à un niveau acceptable.

115. Tout traitement de données personnelles remplissant au moins deux critères de cette liste[33] sera présumé soumis à l'obligation de réaliser une AIPD :

- la collecte de données sensibles ou de données à caractère hautement personnel (catégories de données qui peuvent être considérées comme augmentant le risque d'atteinte aux droits et libertés des personnes, telles que des données de localisation ou des données financières, par exemple) ;
- la collecte de données personnelles à large échelle ;
- le croisement ou la combinaison d'ensembles de données ;
- l'utilisation innovante ou l'application de nouvelles solutions technologiques ou organisationnelles.

116. Les données de localisation sont généralement considérées comme des données hautement personnelles dans la mesure où elles sont susceptibles de révéler des habitudes de vie (déplacements, lieux fréquentés, etc.) et permettent d'inférer de nombreuses informations (les centres d'intérêts, par exemple).

117. Dès lors qu'elles sont collectées à grande échelle, ou qu'elles peuvent être croisées ou combinées à d'autres données, le traitement de données de localisation nécessitera donc une AIPD.

Les mesures à prendre en fonction des résultats de l'AIPD

Une fois le niveau de risque identifié, il convient de concevoir dans l'AIPD un ensemble de mesures visant à le réduire et à le maintenir à un niveau acceptable. Ces mesures doivent notamment intégrer les recommandations de la CNIL[34].

En ce qui concerne spécifiquement les données de localisation, les mesures suivantes peuvent être envisagées :

- **des mesures de sécurité,** telles que le chiffrement des données, le cloisonnement des données en fonction des risques et l'authentification des utilisateurs, la suppression automatique des données dont la durée de conservation est échue ;
- **des mesures de minimisation**, telles qu'une collecte moins fréquente des données, une précision moins exacte et/ou une conservation moins longue (par exemple, uniquement la dernière position) ;
- **des mesures d'anonymisation ou de pseudonymisation ;**

[33] Voir en ce sens les Lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est « susceptible d'engendrer un risque élevé » aux fins du règlement (UE) 2016/679, accessibles sous ce lien : https://www.cnil.fr/fr/publication-des-lignes-directrices-du-g29-sur-les-dpia.

[34] Voir notamment AIPD – Les bases de connaissances, cnil.fr (accessible sous ce lien : https://www.cnil.fr/sites/cnil/files/atoms/files/cnil-pia-3-fr-basesdeconnaissances.pdf)

- **des mesures de protection des données dès la conception :** par exemple en ayant recours à des outils qui effectuent les traitements en local et ne remontent que les données pertinentes en dehors du véhicule (par exemple, une alerte en cas de franchissement d'une zone identifiée, les données de localisation étant uniquement collectées par le dispositif et supprimées après leur traitement) ;
- **des mesures organisationnelles,** telles que l'encadrement et la limitation de l'accès aux bases de données, la limitation de l'accès aux données par les tiers et les sous-traitants, et la mise en place d'un système de traçabilité des actions effectuées afin d'identifier et d'expliquer les comportements anormaux ;
- **des mesures prévoyant une documentation interne,** comme la rédaction d'une charte informatique et la contractualisation des mesures techniques et organisationnelles de sécurité, etc.

118. Ces mesures doivent être sélectionnées au cas par cas afin de réduire les risques spécifiques au traitement de données considéré. Elles doivent être intégrées dans un plan d'action et faire l'objet d'un suivi.

4. FOCUS – L'anonymisation des données de localisation

119. L'anonymisation de données personnelles consiste à utiliser un ensemble de techniques de façon à ce qu'une personne physique ne soit pas identifiable par des moyens raisonnables.

120. Pour démontrer que des données sont anonymes, une analyse de réidentification doit être menée et conclure que le risque d'identification d'une personne est négligeable. A défaut, les données sont à considérer comme demeurant des données personnelles et **restent donc dans le champ d'application du RGPD**.

121. Pour mener cette analyse, les acteurs peuvent se fonder sur l'**avis 05/2014 du G29 sur les techniques d'anonymisation** [35]. De nouvelles lignes directrices sur l'anonymisation sont actuellement en cours d'élaboration au sein du CEPD.

122. L'anonymisation des données de localisation est particulièrement délicate, la CNIL recommande pour ce faire de choisir et combiner, en fonction des cas d'usage, plusieurs techniques adaptées (voir 5.1). Elle recommande en outre, de tenir compte les principales « attaques » en réidentification auxquelles les données de localisation sont exposées (voir 5.2).

Rappel

L'anonymisation de données personnelles constitue un traitement soumis au RGPD. Comme tout traitement, il doit donc respecter les obligations prévues par le RGPD. Notamment :

- Les personnes concernées doivent être individuellement informées du traitement d'anonymisation des données sous réserve des exceptions lorsque celles-ci sont applicables (article 14.5 du RGPD). Dans ce dernier cas, une information générale (par exemple, sur le site web de la société) peut suffire. Le traitement d'anonymisation doit reposer sur une **base légale, au sens de l'article 6 du RGPD**.
- Lorsque ce traitement est fondé sur la base légale de l'intérêt légitime (article 6(1) f. du RGPD), l'anonymisation et l'effacement immédiats des données initiales constituent des facteurs positifs dans la mise en balance des intérêts. En effet, l'utilisation de données anonymisées permet de réduire les risques pour la vie privée et la sécurité des personnes concernées.
- Les **droits des personnes concernées doivent être respectés**. Si le traitement est fondé sur l'intérêt légitime (article 6.1.f du RGPD) ou sur l'exécution d'une mission d'intérêt public (article 6.1.e du RGPD), la personne concernée a notamment le droit de s'opposer au traitement à tout moment, pour des raisons tenant à sa situation particulière.
- Chaque étape du traitement doit être **nécessaire et proportionnée** pour garantir l'anonymat des données finales, conformément au principe de minimisation. Ce, en particulier lorsque le traitement implique la création de nouvelles données personnelles par déduction à partir des données initiales.

Cependant, l'anonymisation des données est un traitement particulièrement peu intrusif, puisqu'il fait disparaître le caractère personnel de la donnée. Si seule la donnée anonymisée est conservée, cette mesure est protectrice de la vie privée. Il convient d'en tenir compte pour apprécier les différentes obligations du RGPD.

4.1 Recommandations techniques spécifiques à l'anonymisation de données de localisation

Recommandations générales

123. Lorsque la finalité du traitement le permet, la CNIL recommande de traiter des données de localisation anonymisées plutôt que des données brutes ou minimisées.

[35] Avis 05/2014 sur les Techniques d'anonymisation adopté le 10 avril 2014, G29, accessible sous ce lien : https://www.cnil.fr/sites/cnil/files/atoms/files/wp216_fr.pdf.

124. La CNIL recommande également d'effectuer le traitement d'anonymisation des données de localisation le plus en amont possible de la collecte des données. Lorsque cela est techniquement possible, il est de même préférable d'anonymiser les données localement, par exemple directement dans le véhicule.

125. Les données de localisation constituent une catégorie de données dont l'anonymat n'est généralement **pas garanti** par le simple fait de **supprimer les identités des personnes** concernées ou par le chiffrement partiel de certains attributs.

126. En outre, il convient de **ne pas considérer la pseudonymisation** de données de localisation comme un moyen suffisant d'assurer une protection adéquate des personnes concernées contre les tentatives d'identification.

Les techniques d'anonymisation

127. Il existe différentes familles de techniques d'anonymisation telles que les techniques de **généralisation, d'agrégation, de perturbation aléatoire** et relatives aux **données synthétiques**.

128. L'**avis du G29 sur les techniques d'anonymisation**[36] décrit ces principales techniques d'anonymisation utilisées aujourd'hui, ainsi que des exemples de jeux de données considérés à tort comme anonymes.

129. Il est important de signaler qu'il n'existe **pas de solution universelle pour l'anonymisation** des données personnelles, et plus spécifiquement pour les données de localisation. Le choix d'anonymiser ou non les données ainsi que la sélection d'une seule ou d'une combinaison de techniques d'anonymisation doit se faire au cas par cas selon les contextes d'usage et de besoin.

130. Le choix de ces techniques doit être documenté et régulièrement réévalué afin de s'assurer que l'anonymisation des données perdure dans le temps.

Différentes techniques d'anonymisation

La **généralisation** consiste à rendre les données moins précises afin que les valeurs soient communes à plusieurs lignes (ou personnes). Elle peut consister par exemple à remplacer des données de localisation brutes par des cellules géographiques prédéfinies, d'une taille adaptée à la densité de circulation.

L'**agrégation** consiste à combiner des données correspondant à plusieurs lignes (ou personnes), par exemple en cumulant des positions de véhicules dans pour établir des « cartes de chaleur » sur une journée.

Les **perturbations aléatoires** consistent à ajouter un bruit aux données, par exemple en modifiant les données de localisation de sorte à ce qu'il ne soit plus possible de reconstituer des trajets individuels.

Les **données synthétiques** sont des jeux de données qui ne correspondent pas à des données de personnes réelles mais dont les propriétés statistiques visent en général à reproduire celles de données réelles. Elles peuvent être purement fictives, être issues d'une modélisation statistique ou être engendrées à partir de données réelles, après un traitement susceptible de combiner des techniques de généralisation, d'agrégation et de perturbation aléatoires.

L'analyse de réidentification

131. L'avis du G29 sur les techniques d'anonymisation fournit un cadre simplifié d'analyse dont les critères rappelés ci-dessous recouvrent les risques les plus connus pour la réidentification des personnes.

132. Pour montrer qu'un jeu de données est anonyme, l'avis considère comme suffisant de montrer que ce jeu de données résiste aux tentatives d'attaques par **individualisation, corrélation et inférence**. Cela signifie qu'il faut cumulativement être en capacité de démontrer qu'il n'est pas possible :

- **d'isoler/d'individualiser** des informations relatives à un seul individu (est-il possible de distinguer une ou plusieurs données relatives à un individu ?)

[36] Avis 05/2014 sur les Techniques d'anonymisation adopté le 10 avril 2014. Accessible sous ce lien : https://www.cnil.fr/sites/cnil/files/atoms/files/wp216_fr.pdf.

- **de relier/corréler** les données d'un même individu ou groupe d'individus (est-il possible de relier les données concernant un individu avec d'autres données du même jeu de données ou avec une autre base de données ?)
- **de déduire/d'inférer** d'un ensemble d'attributs la valeur d'un autre attribut (est-il possible de déduire de nouvelles données relatives aux individus concernés ?)

133. Il est possible, de manière alternative, de réaliser une **analyse *ad hoc* des risques de réidentification.** L'analyse *ad hoc* est plus ouverte que la démonstration des 3 critères de l'avis du G29 : elle sera plus utile pour des données pour lesquels les 3 critères sont difficiles à appliquer (par exemple pour des données non structurées ou non tabulaires). En conclusion de cette analyse, ces **risques de réidentification doivent être négligeables** pour conclure au caractère anonyme des données.

Analyse *ad hoc* des risques de réidentification : comment la faire ?

Les mesures techniques et organisationnelles de sécurité du traitement ne garantissent pas en elles-mêmes l'anonymat d'un jeu de données. De même, les garanties juridiques et contractuelles ne peuvent pas remplacer l'utilisation des techniques d'anonymisation.

Ces mesures et garanties peuvent néanmoins aider à minimiser le risque de réidentification en complément de :

- l'étude des attaques possibles de réidentification dans la littérature scientifique ;
- les facteurs influant le succès de ces attaques ;
- l'étude des moyens raisonnables pouvant être mis en œuvre par un attaquant.

134. Les résultats de l'analyse en réidentification doivent également être documentés et réévaluées en fonction des nouvelles techniques d'attaques et des nouvelles connaissances concernant l'anonymisation.

Exemple de cas d'usage relatif à l'anonymisation

La réalisation d'une carte thermique (« *heat map* » en anglais) peut être une méthode permettant d'anonymiser des données de localisation tout en conservant des informations utiles pour l'analyse. Une carte thermique représente la densité de données de localisation en utilisant des couleurs ou des intensités pour indiquer la concentration de points de données dans une zone géographique donnée.

Prenons l'exemple d'un gestionnaire de flotte qui souhaite optimiser les recharges électriques de ces véhicules sans compromettre la confidentialité des trajets de ces clients. Au lieu de montrer les trajets individualisés, le gestionnaire peut créer une carte thermique où les différents points des trajets, sélectionnés selon des critères adéquats, sont généralisés et agrégés dans des zones différentes, sans montrer l'origine et la destination, et chaque zone est représentée par une intensité de couleur. Les zones ayant eu un grand nombre de points apparaîtront en couleurs plus intenses, tandis que les zones avec moins de points seront en couleurs plus claires. Des contraintes au niveau des seuils d'agrégation de données (nombre de points, période temporelle prise en compte) devront cependant être définies en amont afin de limiter les possibles réidentifications de clients en raison d'un trop faible nombre de points.

Cette méthode permet ainsi d'obtenir des informations précieuses sur les tendances de trajets sans révéler les trajets spécifiques des clients. Les analystes peuvent identifier les zones à forte densité de véhicules, optimiser la localisation des recharges électriques et améliorer l'autonomie des véhicules sans compromettre la confidentialité des données personnelles.

4.2 Réidentification de personnes à partir de données de localisation : les scénarios à prendre en compte

135. Un projet de réidentification par localisation, commencé au Laboratoire d'Innovation numérique de la CNIL (LINC) en 2022 et terminé en 2023, a prouvé qu'une réidentification quasi-automatique d'individus peut être

réalisée à partir de données récupérées chez des courtiers en données (« data-brokers »)[37][38]. Ces résultats sont bien entendu applicables également à d'autres jeux de données contenant des données de localisation.

136. Ce projet de réidentification constitue un exemple intéressant **des différentes attaques,** issues des critères du G29 abordés précédemment, pouvant exister sur un jeu de données résultant d'un mauvais processus d'anonymisation. En l'espèce, le jeu de données était constitué de données pseudonymisées comprenant des données de localisation.

137. Une **attaque par individualisation** peut permettre par exemple de retrouver des « traces » de localisation à partir du jeu de données se rapportant donc à un même individu au sein d'un jeu de données plus large, sur la seule base de la localisation et de l'horodatage des traces.

138. Une **attaque par inférence** peut permettre par exemple de déduire des points d'intérêt, tels que le lieu de domicile et lieu de travail des personnes dont les traces sont présentes dans le jeu de données.

139. Une **attaque par corrélation** peut permettre par exemple d'associer des jeux de données différents au jeu de données. Ces sources peuvent être ouvertes (disponibles publiquement) ou fermées (uniquement à la disposition de l'attaquant).

[37] « Geo TrouveTous - La réidentification des données : de la théorie au cas pratique », LINC, 2022, URL : https://linc.cnil.fr/geo-trouve-tous-la-reidentification-des-donnees-de-la-theorie-au-cas-pratique

[38] « GeoTrouveTous - projet de réidentification par localisation », LINC, 2023, URL : https://linc.cnil.fr/geotrouvetous-projet-de-reidentification-par-geolocalisation

5. Recommandations spécifiques à certaines finalités

5.1 Finalités communes à la gestion de flottes commerciales et à l'utilisation d'un véhicule personnel

L'usage de la localisation pour la lutte contre le vol

140. En cas de vol présumé ou avéré, l'exploitation de la localisation peut permettre d'identifier le lieu d'emplacement du véhicule ou de déterminer une zone où opérer les recherches. Il est donc fréquent que des véhicules soient équipés d'un dispositif (boitier télématique, capteur GPS intégré au véhicule, etc.) qui collecte la localisation du véhicule pour la finalité de lutte contre le vol.

141. Ce traitement de données est généralement mis en œuvre par les gestionnaires de flotte (5.1.1) mais peut également être proposé, en tant que service, aux propriétaires de leurs véhicules (5.1.2) par divers acteurs.

Le cas du gestionnaire de flotte de véhicules loués

Déterminer les rôles de chaque acteur

142. Le gestionnaire de flotte de véhicule loués est le responsable du traitement dès lors :

- que le gestionnaire décide de traiter les données de localisation afin de retrouver le véhicule disparu le plus rapidement possible (dans le cadre de la lutte contre le vol) ;
- qu'il détermine les moyens du traitement et notamment les données collectées, les moyens techniques utilisés pour collecter ces données, la fréquence de la collecte ainsi que la durée de conservation.

Exemple

Il arrive qu'une autorité organisatrice de la mobilité (AOM) recourt à une société privée, dans le cadre d'une délégation de service public, pour organiser un service de location de véhicules à des tarifs préférentiels afin de favoriser les mobilités douces sur son territoire. L'AOM et la société peuvent être considérées comme responsables conjoints du traitement des données de localisation à des fins de lutte contre le vol, lorsqu'elles décident ensemble de la finalité de lutte contre le vol et des moyens du traitement pour cette finalité.

143. Il arrive que le gestionnaire de flotte recoure à un prestataire lui fournissant une plateforme de lutte contre de vol reposant sur le traitement des données de localisation des véhicules de son parc. Dans cette situation, le prestataire, lorsqu'il agit pour le compte, sur instruction et sous l'autorité du gestionnaire de flotte, doit être considéré comme un sous-traitant au sens de l'article 4.8 du RGPD (par exemple, lorsque le prestataire héberge les données de localisation et les transmets au gestionnaire de flotte en cas de vol d'un de ses véhicules).

144. Dans certaines hypothèses, le gestionnaire de flotte récupère directement les données du véhicule connectées pour obtenir sa localisation, notamment à des fins de lutte contre le vol. Ces données, collectées par le constructeur du véhicule, peuvent lui être mises à disposition par le biais d'une API : dans ce cas, le constructeur et le gestionnaire de flotte sont des responsables de traitement distincts et traitent les données de localisation pour des finalités qui leurs sont propres.

Identifier les bases légales mobilisables

Applicabilité de l'article 82 de la loi Informatique et Libertés

145. Pour collecter et traiter les données de localisation, le gestionnaire de flotte est amené à **accéder à des informations stockées dans un terminal** et notamment aux données du boitier télématique dont est équipé le véhicule.

146. L'accès à ces informations **nécessite donc le consentement de l'utilisateur** (le client, locataire du véhicule) sauf lorsque cet accès est nécessaire à la fourniture d'un service expressément demandé par l'utilisateur.

POINT DE DÉBAT

La CNIL s'est interrogée sur l'application de la règle posée par l'article 82 de la loi Informatique et Libertés dans le contexte de la lutte contre le vol du véhicule loué.

L'exigence du consentement du client, qui découle de cette disposition, est susceptible de poser des difficultés dès lors qu'un refus priverait le gestionnaire de flotte d'un moyen efficace de lutte contre le vol.

Pour autant, conditionner la fourniture du service de location au consentement du client à l'accès aux données de localisation afin de lutter contre le vol, risque de porter atteinte à la liberté du consentement.

Face à cette situation, la CNIL a identifié deux interprétations possibles, non exclusives l'une de l'autre, qu'elle souhaite soumettre à consultation publique afin de recueillir des réactions et analyses qui permettront d'éclairer les débats du Collège.

Interprétation 1

Le consentement du client n'est pas requis pour la localisation du véhicule aux fins de lutte contre le vol lorsque :

- La localisation du véhicule a lieu, au cours de la location, uniquement pour d'autres finalités ;
- Après le vol, le même dispositif de localisation du véhicule peut continuer à être utilisé pour faciliter la recherche du véhicule, ainsi que les données de localisation déjà collectées durant l'exécution du contrat. En effet, une fois le véhicule volé, le recueil de la localisation du véhicule ne peut pas être regardé comme une opération de lecture du terminal de *l'utilisateur* du véhicule, au sens de l'article 82 de la loi Informatique et libertés, dès lors que les données se rapportent à un tiers, qui a volé le véhicule, et qui n'est pas l'utilisateur légitime et connu du véhicule. Même dans le cas où le voleur du véhicule s'avérerait être le locataire initial, cette personne ne peut plus être regardée comme l'utilisateur légitime du terminal pour l'application de l'article 82 de la loi et son consentement à ce titre n'est donc pas requis.

Interprétation 2

Le consentement du client est requis dans toutes les autres hypothèses car la localisation du véhicule aux fins de lutte contre le vol n'est pas un service expressément demandé par l'utilisateur mais un traitement mis en place par le loueur du véhicule dans un intérêt économique.

Par exemple, le consentement peut être recueilli par le gestionnaire de flotte au moment de la signature du contrat de location.

Toutefois, le gestionnaire de flotte peut conditionner la localisation de son véhicule à l'acceptation, par le client, de l'accès aux données de localisation afin de lutter contre le vol de ses véhicules lorsqu'il n'identifie pas d'autres moyens de parvenir efficacement à l'objectif poursuivi. Le client, dûment informé **le plus en amont possible** de ce traitement, conserve la liberté de louer ou non le véhicule.

Le gestionnaire de flotte doit demeurer attentif à garantir la liberté du consentement du client[39]. A ce titre, il peut proposer des solutions alternatives en cas de refus de la localisation par ce dernier. Il peut s'agir, par exemple, de l'augmentation de la franchise prévue au contrat en cas de vol (augmentation du montant de la caution prélevée sur la carte de crédit du client), sous réserve du caractère raisonnable, du fait de proposer au client un véhicule de moindre valeur.

---

[39] CJUE, arrêt du 4 juillet 2023, C-252-21, CURIA, URL : https://curia.europa.eu/juris/document/document.jsf?text=&docid=275125. Voir notamment le point 150 : « *Ainsi, ces utilisateurs doivent disposer de la liberté de refuser individuellement, dans le cadre du processus contractuel, de donner leur consentement à des opérations particulières de traitement de données non nécessaires à l'exécution du contrat sans*

Bases légales mobilisables au titre du RGPD

147. Compte tenu de la nécessité de collecter un consentement au sens de l'article 82 de la loi Informatique et Libertés, le consentement (article 6.1.a du RGPD) est généralement la base juridique la plus appropriée pour fonder le traitement de données personnelles effectué à la suite de l'opération de lecture ou d'écriture. Les deux consentements[40] peuvent être collectés simultanément via la même action pour une même finalité (par exemple, en cochant une seule même case indiquant clairement ce à quoi la personne concernée consent).

Appliquer les principes de minimisation et de limitation de la conservation des données

La minimisation des données collectées

148. Si au cours de la location, les données de localisation sont remontées sur des serveurs externes, la CNIL recommande que seule la ou les dernières positions du véhicule soit conservées pour la finalité de lutte contre le vol, chaque donnée de localisation collectée venant écraser la donnée précédente[41].

149. Par ailleurs, dans cette situation, l'accès, au sein du serveur, à la localisation pour cette finalité, est conditionné à la survenance de l'événement redouté (le vol du véhicule suspecté ou avéré), constitutive du fait générateur.

150. Dans le cas contraire, lorsque l'événement redouté se produit, le gestionnaire de flotte peut collecter et remonter des données de localisation sur des serveurs externes afin de lutter contre le vol.

151. **En tout état de cause, dans l'ensemble des situations évoquées, le responsable du traitement doit déterminer la granularité** (par exemple, à l'appui de chiffres, attestant de la proportionnalité de la précision choisie au « taux de découverte » des véhicules) **et la fréquence de la collecte** (par exemple, lorsque le vol est caractérisé, la collecte de plusieurs points de localisation du véhicule peut s'avérer nécessaire pour identifier le lieu d'emplacement du véhicule ou déterminer une zone où opérer les recherches) **en étant en mesure de les justifier.**

La limitation de la conservation des données

152. Deux situations doivent être distinguées :

- **En l'absence de vol du véhicule,** aucune donnée ne doit être conservée à cette fin une fois la location terminée.
- **En cas de vol du véhicule au cours de la location**, les données de localisation ne peuvent être conservées que le temps de l'instruction du dossier par les autorités judiciaires compétentes et les autres tiers impliqués dans la gestion des conséquences du vol ou jusqu'à l'issue d'une procédure de levée de doute n'aboutissant pas à la confirmation du vol du véhicule.

Garantir l'information et l'exercice des droits des personnes concernées

153. Les gestionnaires de flotte sont tenus de respecter les obligations de transparence à l'égard des personnes concernées sur les traitements de données de localisation qu'ils effectuent pour la lutte contre le vol des véhicules.

154. En effet, le client doit recevoir, au moment de la souscription au service de location, une information dédiée. Cette information peut se trouver au sein du contrat de location ou dans une politique de confidentialité dédiée, et être délivrée par voie dématérialisée ou au format papier, selon le mode de souscription.

155. Le client doit être informé par le responsable du traitement :

- que seul le personnel habilité du gestionnaire de flotte ou du prestataire spécialisé a accès à la donnée de localisation ;
- que les données de localisation peuvent être exploitées par les forces de l'ordre dans le cadre de l'enquête sur le vol du véhicule et de l'instruction du dossier par les autorités judiciaires compétentes.

---

qu'ils soient pour autant tenus de renoncer intégralement à l'utilisation du service offert par l'opérateur du réseau social en ligne, ce qui implique que lesdits utilisateurs se voient proposer, le cas échéant contre une rémunération appropriée, une alternative équivalente non accompagnée de telles opérations de traitement de données. »

[40] Le consentement requis en vertu de l'article 82 de la loi « Informatique et Libertés » et le consentement nécessaire comme base juridique pour le traitement de données.

[41] Voir en ce sens : Conseil d'État, 10ème - 9ème chambres réunies, 06/12/2023, 467368, Inédit au recueil Lebon, Légifrance, URL : https://www.legifrance.gouv.fr/ceta/id/CETATEXT000048527626.

Adopter des mesures de sécurité pour encadrer les traitements de données de localisation

156. Les recommandations générales s'appliquent (voir point 3.9).

157. Plus spécifiquement, les responsables du traitement doivent :

- restreindre la consultation ou l'affichage des données de localisation, de façon que les personnels habilités, ayant besoin de connaître la position d'un véhicule, ne puissent y accéder qu'à la survenance du fait générateur, à savoir la déclaration ou la suspicion d'un vol ;
- encadrer et limiter les accès à cette position aux personnels habilités, en définissant des rôles et les droits qui leurs sont attribués ;
- prévoir une journalisation des accès et des motifs de consultation. Ces motifs doivent être explicitement mentionnés par la personne habilitée lors d'un accès ;
- réaliser une analyse d'impact sur la protection des données (AIPD), dès lors notamment, que les données de localisation sont des données hautement personnelles et qu'elles seront, généralement, traitées à grande échelle.

Le cas du particulier

158. Un particulier peut souscrire, auprès d'une société fournissant un service de lutte contre le vol ou du constructeur, à un service qui permet, grâce à l'exploitation des données de localisation, de localiser le véhicule connecté en cas de vol. Cela peut se faire, par exemple, au moyen d'un dispositif installé au sein du véhicule.

159. La CNIL rappelle que le constructeur ne peut pas conditionner l'achat du véhicule à un tel système : il ne peut s'agir que de service souscrits et activés spécifiquement par l'acheteur.

Déterminer les rôles de chaque acteur

160. La société fournissant un service de lutte contre le vol, ou le constructeur, est le responsable du traitement dès lors :

- qu'il décide de traiter les données de localisation afin de retrouver le véhicule disparu le plus rapidement possible (dans le cadre de la lutte contre le vol) ;
- qu'il détermine les moyens du traitement et notamment les données collectées, les moyens techniques utilisés pour collecter ces données, la fréquence de la collecte ainsi que la durée de conservation.

Identifier les bases légales mobilisables

Applicabilité de l'article 82 de la loi Informatique et Libertés

161. En ce qui concerne l'accès aux données de localisation pour la finalité de « lutte contre le vol », **le consentement de l'usager n'est pas requis** car cet accès est nécessaire à la fourniture du service. En effet, l'accès aux données de localisation du véhicule est nécessaire à la fourniture du service payant de pistage (ou « *tracking* ») qui est demandé par le client.

Base légale mobilisable au titre du RGPD

162. L'exécution d'un contrat constitue une base juridique adaptée pour le traitement des données de localisation.

Appliquer les principes de minimisation et de limitation de la conservation des données

La minimisation des données collectées

163. Si au cours du trajet du véhicule, les données de localisation sont remontées sur des serveurs externes, la CNIL recommande que seule la ou les dernières positions du véhicule soient conservées pour la finalité de lutte contre le vol, chaque donnée de localisation collectée venant écraser la donnée précédente. Dans cette situation, l'accès à la localisation, au sein des serveurs, pour cette finalité est conditionné à la survenance de l'événement (le vol du véhicule suspecté ou avéré), constitutive du fait générateur.

164. Dans le cas contraire, lorsque l'événement se produit, le responsable du traitement peut collecter et remonter des données de localisation sur des serveurs externes pour la finalité de lutte contre le vol.

165. **En tout état de cause, dans l'ensemble des situations évoquées, le responsable du traitement doit déterminer la granularité** (par exemple, à l'appui de chiffres, attestant de la proportionnalité de la précision choisie au « taux de découverte » des véhicules) **et la fréquence de la collecte** (par exemple, lorsque le vol est caractérisé, la collecte de plusieurs points de localisation du véhicule peut s'avérer nécessaire pour identifier le lieu d'emplacement du véhicule ou déterminer une zone où opérer les recherches) **en étant en mesure de les justifier.**

La limitation de la conservation des données

166. **En cas de vol du véhicule,** les données de localisation ne peuvent être conservées que le temps de l'instruction du dossier par les autorités judiciaires compétentes ou par les tiers impliqués dans la gestion des suites du vol, ou jusqu'à l'issue d'une procédure de levée de doute n'aboutissant pas à la confirmation du vol du véhicule.

Garantir l'information des personnes concernées

167. Le particulier ayant souscrit au service doit être informé par le responsable du traitement :

- que seul le personnel habilité de la société fournissant un service de lutte contre le vol ou du constructeur, a accès à la donnée de localisation ;
- que les données de localisation peuvent être exploitées par les forces de l'ordre dans le cadre de l'enquête sur le vol du véhicule.

168. Ces informations peuvent, par exemple, être fournies à la signature du contrat.

L'usage de la localisation pour l'assistance aux personnes en cas d'accident

169. Les données de localisation peuvent s'avérer utiles pour prêter assistance aux personnes victimes d'un accident de la circulation (par exemple, une assistance médicale ou de premiers secours) afin de permettre d'identifier avec précision le lieu de sa survenance.

170. **Certains acteurs, tels que les gestionnaires de flotte, proposent des services d'assistance en cas d'accident à leurs clients.** Ces services peuvent reposer sur l'installation d'un dispositif connecté ou en lien avec une application mobile, afin d'identifier la localisation du véhicule au moment de cet accident.

171. **De tels services sont également proposés directement aux particuliers** dans le cadre de l'usage de leur véhicule personnel (cyclistes, motocyclistes), qui peuvent s'équiper d'objets connectés dédiés (par exemple, un casque connecté), en lien, parfois, avec une application mobile afin d'obtenir une assistance en cas d'accident (par exemple, si l'objet connecté détecte une chute). La présente recommandation concerne les deux usages.

172. Seuls ces dispositifs d'assistance d'urgence sont concernés par les recommandations qui suivent. Ils doivent être différenciés du système eCall embarqué fondé sur le service 112.

Le système eCall embarqué fondé sur le service 112

La règlementation européenne[42] a imposé, pour toutes les voitures particulières fabriquées après le 31 mars 2018, un système dénommé « eCall » embarqué fondé sur le numéro 112 (numéro d'appel d'urgence européen). En cas d'accident grave sur le territoire de l'Union européenne, le véhicule déclenche automatiquement un appel « eCall » vers le 112, qui permet d'envoyer les secours sur les lieux de l'accident[43] (la localisation du véhicule est exploitée dans cadre).

Les lignes directrices 01/2020 du CEPD sur le traitement des données à caractère personnel dans le contexte des véhicules connectés et des applications liées à la mobilité[44] contiennent une étude de cas consacrée au dispositif eCall à laquelle les professionnels et les particuliers peuvent se référer.

Les véhicules des gestionnaires de flottes étant régulièrement renouvelés, leurs utilisateurs bénéficient, dans l'immense majorité, du dispositif obligatoire eCall.

---

[42] Règlement (UE) 2015/758 du 29 avril 2015 concernant les exigences en matière de réception par type pour le déploiement du système eCall embarqué fondé sur le service 112 et modifiant la directive 2007/46/CE, EUR-Lex, URL : https://eur-lex.europa.eu/eli/reg/2015/758/oj/fra.

[43] Le générateur eCall installé à l'intérieur du véhicule, qui permet la transmission par l'intermédiaire d'un réseau public de communications mobiles, envoie un appel d'urgence, qui est déclenché automatiquement grâce aux capteurs du véhicule ou manuellement par les occupants du véhicule uniquement en cas d'accident. Outre l'activation de la communication audio, en cas d'accident, un ensemble minimal de données est automatiquement généré (incluant la dernière position connue du véhicule - latitude et longitude -) et envoyé au centre de réception des appels d'urgence.

[44] Lignes directrices 01/2020 sur le traitement des données à caractère personnel dans le contexte des véhicules connectés et des applications liées à la mobilité, CEPD, URL : https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-012020-processing-personal-data-context_fr.

La réglementation européenne autorise également le recours à des systèmes embarqué alternatifs[45] au système « eCall » embarqué fondé sur le numéro 112. Les échanges avec le secteur n'ont pas permis d'identifier l'usage de tels dispositifs, le cas échéant, ceux-ci devraient être conformes à la réglementation en vigueur[46].

Déterminer les rôles de chaque acteur

173. Plusieurs cas de figure peuvent se présenter selon que la prestation d'assistance en cas d'accident est prise en charge directement par la société qui commercialise le dispositif en question ou que celle-ci est externalisée auprès d'une société en charge de la prestation.

Cas 1 : la prestation d'assistance est opérée directement par la société qui commercialise le dispositif.

174. La société qui commercialise le dispositif est le responsable du traitement dès lors :

- qu'elle décide de traiter les données de localisation afin de permettre l'exécution de la prestation d'assistance à laquelle l'utilisateur a souscrit ;
- qu'elle détermine les moyens du traitement et notamment les données collectées, les moyens techniques utilisés pour collecter ces données, la fréquence de la collecte ainsi que la durée de conservation.

Cas 2 : la prestation d'assistance est opérée par une société en charge de la prestation d'assistance distincte de la société qui commercialise le dispositif.

175. La société qui commercialise le dispositif peut faire le choix d'externaliser la prestation d'assistance en la confiant à une société en charge de la prestation d'assistance qui sera destinataire des données de localisation.

176. Les données de localisation peuvent alors soit :

- **être directement collectées par la société en charge de la prestation d'assistance :**

  Dans cette situation, le fournisseur du dispositif n'assure que la commercialisation du dispositif et le service d'assistance est intégralement fournit par la société en charge de la prestation d'assistance. Cette dernière doit être considérée comme le responsable du traitement dès lors qu'elle décide de traiter les données de localisation afin de permettre l'exécution de la prestation d'assistance dont elle a la charge, détermine la fréquence de la collecte ainsi que la durée de conservation des données.

- **être collectées par la société qui commercialise le dispositif puis transmises à la société en charge de la prestation d'assistance avec laquelle elle entretient une relation contractuelle :**

  La société qui commercialise le dispositif et la société en charge de la prestation d'assistance pourront être considérées comme responsables conjoints du traitement si elles ont décidé ensemble de traiter les données de localisation afin de permettre l'exécution de la prestation d'assistance et déterminé les moyens essentiels du traitement notamment, le moment et la fréquence de la collecte ainsi que la durée de conservation.

  Dans ce cas, chaque responsable du traitement doit évaluer l'étendue de son niveau de responsabilité, les acteurs n'étant pas nécessairement responsables des mêmes opérations du traitement. En effet, leur responsabilité peut varier en fonction de leur implication sur les opérations du traitement pour la finalité définie en commun.

  A défaut, la société qui commercialise le dispositif peut être considérée comme un sous-traitant si elle agit au nom et pour le compte de la société en charge de la prestation d'assistance.

[45] *Ibid.*

[46] *Ibid.*

Exemple

Dans le cadre de la commercialisation d'un équipement de sécurité connecté (par exemple, un casque de motocycliste), le fabricant et le prestataire d'assistance décident conjointement de traiter les données de localisation afin de permettre l'exécution d'une prestation d'assistance en cas d'accident impliquant le porteur du casque. Le fabricant peut décider des moyens techniques utilisés pour collecter la donnée de localisation, le choix du prestataire, les modalités de récupération et de transmission des données ainsi que le moment et la fréquence de la collecte. La société en charge de la prestation d'assistance détermine pour sa part, les personnes qui ont accès aux données, leur durée de conservation, etc. Le fabricant et le prestataire d'assistance sont responsables conjoints du traitement.

177. En pratique, quel que soit le scénario retenu, le responsable du traitement pourra être amené à mettre en relation la personne concernée avec les services de secours ou à prévenir directement ces derniers en leur transmettant, si nécessaire, les informations de localisation notamment, aux fins d'optimiser leur intervention et la prise en charge de la personne concernée.

Identifier les personnes concernées

178. La personne concernée est celle qui utilise le dispositif connecté intégrant le service d'assistance d'urgence, qu'elle en soit propriétaire (par exemple, un cycliste détenteur d'un casque connecté dans le cadre de ses déplacements à titre privé), utilisateur ou locataire (par exemple, le conducteur d'un scooter en location, identifié dans le contrat de location).

Identifier les bases légales mobilisables

Applicabilité de l'article 82 de la loi Informatique et Libertés

179. Pour collecter et traiter les données de localisation, la société qui commercialise le dispositif ou le cas échéant, la société en charge de la prestation d'assistance, est amenée à **accéder à des informations stockées dans un terminal** : accès aux données des dispositifs ou objets connectés.

180. L'accès à ces informations **nécessite le consentement de l'utilisateur** (la personne utilisatrice du dispositif ou objet connecté intégrant le service d'assistance d'urgence) **sauf lorsque cet accès est nécessaire à la fourniture du service expressément demandé par l'utilisateur**.

181. En ce qui concerne l'accès aux données de localisation à des fins d'assistance aux personnes en cas d'accident dans le cadre de la location d'un véhicule ou de l'achat d'un véhicule :

- Soit ce service fait l'objet d'une clause contractuelle ad hoc, optionnelle, ou d'un contrat spécifique lors de l'achat ou de la location et les données sont alors nécessaires à ce service spécifique, souscrit par le client ; un consentement, au titre de l'article 82 de la loi Informatique et libertés n'est pas requis ;
- Soit ce service est automatiquement associé par le responsable du traitement à l'achat ou à location du véhicule ; dans ce cas, le traitement ne peut être regardé comme nécessaire au service qui est demandé par l'utilisateur car il en constitue un accessoire détachable ; un consentement est requis au titre de l'article 82 de la loi Informatique et Libertés et, s'il est refusé, le service ne doit pas être activé.

182. Lorsque la personne concernée achète un objet connecté dédié (par exemple, un casque connecté), le consentement de l'utilisateur n'est pas requis dès lors que l'accès aux données de localisation, et leur traitement, est nécessaire à la fourniture du service.

Base légale mobilisable au titre du RGPD

183. Le responsable du traitement demeure responsable du choix, au cas par cas, de la base légale pour ses traitements de données et devra être en mesure de le justifier.

184. Si l'assistance constitue une prestation optionnelle du responsable du traitement à la vente du véhicule, de l'objet connecté ou à la location du véhicule alors la base légale du contrat (article 6.1.b du RGPD) peut être mobilisée pour le traitement des données de localisation à cette fin.

Point d'attention

Si la prestation d'assistance fait partie des prestations de base incluses dans le contrat de vente ou de location souscrit par le client sans que le client n'ait la possibilité de la refuser, l'exécution du contrat ne constitue pas une base juridique pertinente pour le traitement des données de localisation, l'objectif principal du contrat étant la vente du véhicule ou la fourniture du service de location au client final. Si le traitement des données de localisation est utile à la poursuite de la finalité d'assistance et de dépannage, il n'apparaît pas nécessaire à l'objet même du contrat, la vente ou location du véhicule pouvant être effectuée sans que ce traitement soit mis en œuvre.

Dans cette hypothèse, le gestionnaire de la flotte peut se fonder sur le consentement (article 6.1.a du RGPD) pour le traitement des données de localisation pour la finalité de d'assistance aux personnes et de dépannage du véhicule, dès lors que ce consentement devra être recueilli au titre de l'article 82 de la loi « Informatique et libertés ». Les deux consentements peuvent être recueillis ensemble.

Appliquer les principes de minimisation et de limitation de la conservation des données

La minimisation des données collectées

185. Le responsable du traitement doit déterminer la granularité et la fréquence de la collecte.

186. La CNIL recommande de collecter et de remonter la localisation du véhicule au moment de la survenance de l'accident, constitutif du fait générateur. Il appartient au responsable du traitement de démontrer, au cas par cas, la nécessité de collecter les données de localisation ainsi que celle de les remonter sur des serveurs distants avant la survenance de l'accident, notamment s'il existe un risque que les données ne puissent pas être remontées au moment de l'accident.

187. **En tout état de cause,** seules les données nécessaires pour faciliter l'arrivée des secours jusqu'au lieu de l'accident et assurer la prise en charge des victimes doivent être conservées**. Par conséquent, une conservation de l'intégralité des données n'est pas justifiée au regard de la finalité poursuivie.**

188. Par analogie avec le fonctionnement du système eCall embarqué fondé sur le service 112**, la CNIL recommande que seules les trois dernières positions soient conservées** dans la mesure où cela est strictement nécessaire pour préciser la position actuelle du cycle ou du deux-roues motorisé.

189. **En tout état de cause, l'accès et l'exploitation de ces positions pour cette finalité restent conditionnés à la survenance du fait générateur** (par exemple, la chute du conducteur du scooter ou du cycle).

190. Lorsque les données de localisation sont collectées par la société qui commercialise le dispositif puis transmises à la société en charge de la prestation d'assistance, la transmission est conditionnée à la survenance du fait générateur. Lorsque les trois dernières positions apparaissent nécessaires au regard de la finalité, seules ces dernières doivent être transmises à la société en charge de la prestation d'assistance.

La limitation de la conservation des données

191. **En l'absence d'accident,** pour la finalité d'assistance, la conservation des données de localisation au-delà de la fin d'un trajet et en l'absence d'accident n'est pas nécessaire. Par conséquent, celles-ci doivent être supprimées par le responsable du traitement.

192. **En cas d'accident,** les données de localisation doivent être supprimées une fois que la prestation d'assistance a été réalisée ou que les procédures qui y sont liées prennent fin.

Garantir l'information des personnes concernées

193. Le responsable du traitement est tenu de respecter les obligations d'information des personnes concernées sur les traitements de données de localisation qu'il effectue.

194. En effet, **le client propriétaire de l'objet connecté doit recevoir, au moment de l'achat de l'objet connecté, une information dédiée**. Cette information peut se trouver dans la notice d'utilisation du dispositif délivrée par la société qui le commercialise et qui contient une explication sur les traitements de données de localisation pour la finalité d'assistance. En complément, la CNIL recommande, à titre de bonne pratique, l'utilisation d'un QR code apposé sur le dispositif connecté qui renvoie vers une information complète en ligne.

195. Le locataire (par exemple, le conducteur d'un scooter ou d'un cycle en location, identifié dans le contrat de location) **doit recevoir, au moment de la souscription au service de location, une information dédiée**. Cette information peut se trouver au sein du contrat de location ou dans une politique de confidentialité dédiée, et être délivrée soit par voie dématérialisée, soit au format papier, selon le mode de souscription.

196. Lorsque la prestation d'assistance est opérée par une société en charge de la prestation d'assistance distincte de la société qui commercialise le dispositif, l'usager du service doit être informé que les données de localisation collectées par la société qui commercialise le dispositif sont transmises à la société en charge de la prestation d'assistance afin de permettre l'exécution de la prestation d'assistance.

197. En présence de responsables conjoints du traitement, l'accord qui les lie doit prévoir leurs obligations respectives quant à la communication aux usagers du service, des informations visées aux articles 13 et 14 du RGPD.

Adopter des mesures de sécurité pour encadrer les traitements de données de localisation

198. Les recommandations générales s'appliquent (voir point 3.9).

199. Le système eCall basé sur le numéro 112 ainsi que tout autre système eCall géré par des services tiers ou des services à valeur ajoutée doivent être conçus de manière à empêcher l'échange de données personnelles entre ces systèmes, ce qui implique un cloisonnement (réseau, applicatif) des traitements liés à la fonctionnalité eCall.

200. La CNIL recommande, en outre, aux responsables du traitement :

- de restreindre les droits de consultation ou d'affichage aux dernières données de localisation, de façon que les personnels habilités ayant besoin de connaître la position d'un véhicule, ne puissent y accéder qu'à la survenance d'un fait générateur ;
- de limiter les accès à cette position aux personnels habilités, en définissant des rôles et les droits qui leurs sont attribués ;
- de prévoir une journalisation des accès et des motifs de consultation, afin de maîtriser les risques de consultations abusives ou motivées par d'autres finalités ;
- de réaliser une analyse d'impact sur la protection des données (AIPD).

L'usage de la localisation pour l'optimisation et l'amélioration des produits et services

201. L'optimisation et l'amélioration des produits et services **concerne l'ensemble des acteurs de l'écosystème du véhicule connecté** (constructeurs automobiles, équipementiers, loueurs, etc.) **et renvoie à des usages variés** (gestion de flotte et usage propriétaire du véhicule).

202. Ces recommandations visent :

- **L'optimisation et l'amélioration des fonctionnalités du véhicule et de ses équipements.**

> **Exemple 1**
>
> Pour un constructeur automobile, le fait d'améliorer les systèmes de conduite autonome ou d'aide à la conduite.
>
> **Exemple 2**
>
> Pour un équipementier, le fait d'optimiser la durée de vie d'une batterie.

- **La maintenance prédictive** qui consiste à collecter et à analyser, en temps réel, des données propres aux équipements du véhicule afin d'anticiper des problèmes potentiels et d'éviter une panne. Cette finalité nécessite un volume important de données (pseudonymisées) et une profondeur historique pour apprendre et « réapprendre » au cours du temps, en tenant compte d'éventuels biais qui peuvent être identifiés.

> **Exemple**
>
> Pour un équipementier, la prédiction d'usure de pneumatiques.

- **L'amélioration des services connectés ou des services du gestionnaire de flottes.**

> **Exemple**
>
> Un loueur de scooters électriques souhaite connaitre les pratiques des utilisateurs de sa flotte, dont les batteries préchargées sont disponibles pour échange, dans différents espaces physiques répartis sur un territoire déterminé. Les données de localisation anonymisées des trajets effectués lui permettent de mieux prévoir les comportements des utilisateurs ou la durée de vie des recharges utilisées et d'améliorer ainsi le service rendu à ses clients ainsi que la gestion de son parc.

203. **En revanche, le projet de recommandation ne vise pas les traitements de données ayant pour finalité la sécurité du véhicule,** pour laquelle certaines opérations peuvent être opérées à distance et n'impliquent pas de données de localisation (par exemple, quand un constructeur opère une correction télématique des défauts de sécurité[47]).

> **Point d'attention**
>
> **La notion d'optimisation et d'amélioration des produits et services recouvre des réalités variées.**
>
> Le responsable du traitement doit **définir de manière précise la finalité qu'il poursuit à des fins d'optimisation et d'amélioration des produits et services** afin de pouvoir s'assurer ensuite du respect des principes qui en dépendent (notamment la minimisation des données [48] et la limitation de la conservation[49]).

204. L'optimisation et l'amélioration des produits et services peuvent impliquer des traitements de données, y compris de localisation, qui diffèrent d'un acteur à l'autre :

- les données peuvent être collectées **spécifiquement à cette fin** ou **avoir été collectées initialement pour une autre finalité** par le responsable du traitement lui-même (par exemple, dans le cadre de la gestion de flotte) ou par un autre responsable du traitement **et être réutilisées pour cette nouvelle finalité.** Dans ce dernier cas, **cela implique de prendre des précautions complémentaires.**

- **la nature des données concernées peut également varier :** le responsable du traitement peut traiter des données personnelles, principalement pseudonymisées, ou avoir recours à des données anonymisées.

Déterminer les rôles de chaque acteur

205. Un acteur qui a lui-même développé et conçu un produit ou un service peut chercher à l'améliorer ou à l'optimiser pour son bénéfice. Il agit alors dans son propre intérêt et détermine, en général, les finalités et les moyens du traitement. Dans ce cas, il sera responsable du traitement.

> **Exemple 1**
>
> Un constructeur automobile collecte des données issues d'un véhicule connecté pour améliorer, par exemple, son système d'aide à l'automatisation de la conduite (aide au démarrage en côte, système d'arrêt et de redémarrage automatique du moteur, etc.). **Il agit en tant que responsable du traitement** puisqu'il détermine les finalités et les moyens du traitement des données en question.

[47] Article L. 1514-6 du Code des transports.

[48] Article 5(1). c) du RPGD.

[49] Article 5(1). e) du RPGD.

Exemple 2

Un gestionnaire de flotte traite les données de localisation (anonymisées) de ses clients pour optimiser la durée de vie de ses recharges électriques afin d'améliorer la gestion de son parc. **Il agit en tant que responsable du traitement d'anonymisation.** Le traitement des données anonymisées n'est ensuite plus soumis au RGPD.

206. Il se peut que deux ou plusieurs acteurs aient, en commun, développé et conçu un produit ou un service et puissent chercher à l'améliorer ou à l'optimiser. S'ils ont déterminé conjointement les finalités et les moyens du traitement, ils pourront être considérés comme des responsables conjoints du traitement (article 26 du RGPD).

207. Il peut arriver qu'un équipementier (par exemple, un fournisseur de boitier) agissant en qualité de sous-traitant d'un constructeur ou d'un gestionnaire de flotte, responsable du traitement, veuille anonymiser des données issues d'un véhicule connecté afin d'améliorer son équipement (par exemple, un boitier connecté). Il pourra le faire si cette réutilisation des données est compatible avec le traitement initial et que le responsable du traitement lui en a donné l'autorisation[50].

Les conditions de légalité et l'identification des bases légales mobilisables

208. Deux cas doivent être distingués selon que la finalité poursuivie nécessite le traitement de données personnelles ou de données préalablement anonymisées.

A. La finalité d'optimisation et d'amélioration des produits et services nécessite le traitement de données personnelles (y compris pseudonymisées)

❖ *Applicabilité de l'article 82 de la loi Informatique et Libertés*

- **La finalité d'optimisation et d'amélioration des produits et services repose sur une collecte ad hoc de données personnelles par le responsable du traitement**

209. Lorsque le responsable du traitement est amené à accéder à des informations stockées dans un terminal, le consentement préalable des utilisateurs devra être recherché afin de collecter des données personnelles pour cette finalité. En effet, cette finalité n'a pas vocation à faciliter la communication et n'est pas strictement nécessaire à la fourniture d'un service à la demande expresse de l'utilisateur.

- **La finalité d'optimisation et d'amélioration des produits et services implique la réutilisation de données personnelles (y compris pseudonymisées) collectées précédemment pour une autre finalité**

210. Le responsable du traitement peut décider de réutiliser des données personnelles qu'il a collectées pour une finalité initiale : on parle alors de traitement ultérieur de données.

211. Dans ce cas, lorsque les données sont initialement collectées via des opérations de lecture/écriture soumises au consentement de l'utilisateur, en application de l'article 82 de la loi Informatique et Libertés, elles ne peuvent être réutilisées pour une autre finalité, sans anonymisation, qu'**à la condition que l'utilisateur ait donné son consentement libre, spécifique, éclairé et univoque à cette nouvelle finalité[51].**

212. **Le consentement de la personne concernée doit donc être obtenu en amont du traitement ultérieur de données de localisation pour cette finalité.**

[50] Sur ce point, se référer aux recommandations générales, point 3.3.

[51] Voir en ce sens, la délibération SAN-2022-025 du 29 décembre 2022. Accessible sous ce lien : https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000046768989 (paragraphes 58 et suivants). Voir également en ce sens, la délibération de la formation restreinte n°SAN-2022-023 du 19 décembre 2022 concernant la société X. Accessible sous ce lien : https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000046768989 (paragraphes 48 et suivants).

❖ *Analyse sur la base juridique au sens de l'article 6 du RGPD*

213. **Le consentement** (article 6.1.a du RGPD) **constitue généralement la base juridique la plus appropriée pour fonder le traitement de données personnelles effectué à la suite de ces opérations lorsqu'il est requis, en tout état de cause, sur le fondement de l'article 82 de la LIL.**

214. Les deux consentements[52] peuvent être collectés simultanément via la même action pour une même finalité (par exemple, en cochant une seule même case indiquant clairement ce à quoi la personne concernée consent).

B. La finalité d'optimisation et d'amélioration des produits et services repose sur l'anonymisation de données initialement collectées pour une autre finalité

❖ *Applicabilité de l'article 82 de la loi Informatique et Libertés*

215. **Lorsque des données personnelles sont collectées pour une finalité initiale** – que celle-ci soit soumise au consentement des personnes concernées ou, exemptée au titre de l'article 82 de la loi Informatique et Libertés – **leur réutilisation ne nécessite pas de consentement à la condition d'avoir été préalablement anonymisées de manière effective.** En effet, le traitement d'anonymisation des données – lorsque celle-ci est effective – permet une réutilisation des données sans risques pour l'utilisateur[53]**.** Le RGPD reste toutefois applicable au traitement d'anonymisation qui doit donc se fonder sur une base juridique[54], qui est généralement, l'intérêt légitime.

❖ *Analyse sur la base juridique au sens de l'article 6 du RGPD*

216. Lorsque les données personnelles sont initialement collectées pour une autre finalité et sont ensuite anonymisées pour la finalité d'optimisation et d'amélioration des produits et services, le traitement relatif à l'anonymisation des données peut être fondé sur l'intérêt légitime du responsable du traitement (article 6.1.f du RGPD), sous réserve de respecter les critères de validité de cette base juridique.

Point d'attention

La collecte de données personnelles dans le but spécifique de les anonymiser pour la finalité d'optimisation et d'amélioration des produits et services reste soumise au recueil du consentement conformément à l'article 82 de la loi Informatique et Libertés, y compris lorsque le traitement d'anonymisation est opéré à bref délai. Le traitement relatif à l'anonymisation des données peut être fondé sur l'intérêt légitime du responsable du traitement, sous réserve de respecter les conditions de validité (article 6.1.f du RGPD).

Appliquer les principes de minimisation et de limitation de la conservation des données

Rappel

La CNIL recommande aux acteurs de **privilégier les traitements de données de localisation en local**, au sein du véhicule ou du dispositif connecté au véhicule, lorsque cela est pertinent au regard des finalités poursuivies (voir point 3.6).

Dans les **hypothèses où il est nécessaire de remonter les données de localisation** au sein des serveurs du responsable du traitement, ce dernier doit notamment tenir compte des recommandations relatives au cas d'une base de données servant des finalités multiples (voir point 3.6).

---

[52] Le consentement requis en vertu de l'article 82 de la loi Informatique et Libertés et le consentement nécessaire comme base juridique pour le traitement de donnée.

[53] Sur ce point, voir la déclaration 03/2021 sur le règlement «vie privée et communications électroniques» (PDF, 108 ko), pp. 4-5, URL : https://www.edpb.europa.eu/system/files/2021-06/edpb_statement_032021_eprivacy_regulation_fr.pdf : « *L'EDPB tient à souligner que les données susmentionnées peuvent tout de même être traitées sans le consentement de l'utilisateur final et sans risque pour les utilisateurs, une fois qu'elles ont été anonymisées* ».

[54] Sur ce point, se référer aux recommandations spécifiques à l'anonymisation, au point 4 de la recommandation.

La minimisation des données collectées

217. À priori, et sauf démonstration de leur nécessité par le responsable du traitement, les données identifiantes n'apparaissent pas pertinentes pour cette finalité tout comme l'usage de données de localisation précises ou détaillées.

> **Exemple**
>
> Lorsqu'un constructeur ou un gestionnaire de flotte souhaite savoir à quelles fréquences ou dans quelles situations, pour une catégorie de véhicule donné, certains services ou fonctionnalités du véhicule sont activés par son utilisateur, **l'utilisation de données anonymisées afin de produire des statistiques en lien avec la finalité** permet d'atteindre l'objectif poursuivi.

La limitation de la conservation des données

218. Le responsable du traitement doit veiller à définir une durée de conservation limitée. En cas de pseudonymisation, le RGPD continue de s'appliquer et les données ne peuvent être conservées sans limitation de durée. La CNIL estime qu'**une durée de conservation de trois ans** est proportionnée pour la finalité d'optimisation et d'amélioration des produits et services.

219. Une fois anonymisées, les données peuvent être conservées sans limitation de durée.

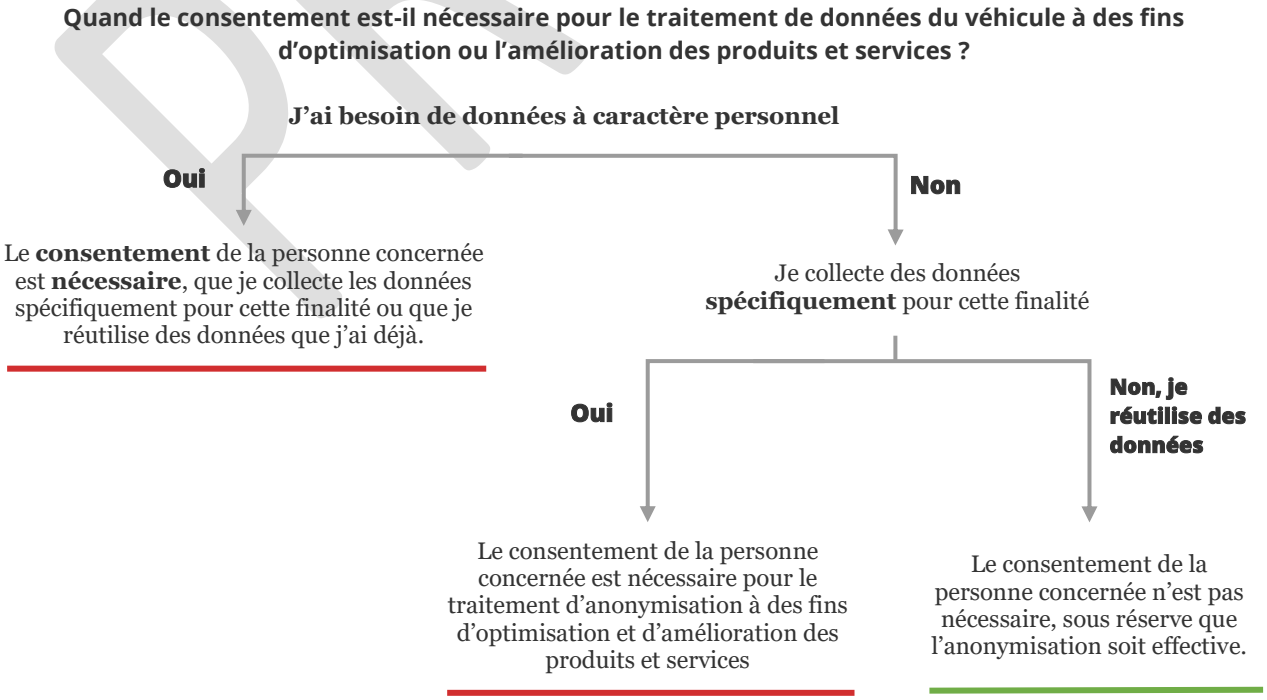
Garantir l'information et l'exercice des droits des personnes concernées

L'information des personnes concernées

220. Au titre de l'obligation de transparence prévue par le RGPD et afin de permettre à l'utilisateur d'exercer une maîtrise effective sur ses données, celui-ci doit être informé des finalités du traitement. La CNIL recommande que le responsable du traitement identifie clairement des données susceptibles d'être traitées en local, directement dans le véhicule, ainsi que de celles qui sortent/sont extraites du véhicule. Un schéma explicitant les données et les flux associés peut être utilement mis à disposition des personnes par exemple, dans le guide d'utilisation du véhicule (physique ou dématérialisé) ou sur le site internet du constructeur automobile ou du gestionnaire de flotte.

L'exercice des droits des personnes concernées

221. Les personnes concernées doivent être spécifiquement informées de l'existence du droit de retirer leur consentement à tout moment, sans porter atteinte à la licéité du traitement fondé sur le consentement effectué avant le retrait de celui-ci.



5.2 Finalités spécifiques à la gestion de flotte commerciale

L'usage de la localisation à des fins de gestion de flotte par les loueurs de véhicules

222. Les loueurs de véhicules, y compris en autopartage, collectent souvent les données de localisation des véhicules loués afin d'assurer la gestion commerciale de leur flotte.

223. Plus précisément, ces traitements poursuivent généralement les finalités suivantes :

- **la gestion de l'exécution des contrats de location,** notamment pour :
  - **organiser la fourniture et la restitution du véhicule** (identifier la localisation du véhicule, avant et à l'issue d'une location ; permettre le verrouillage ou le déverrouillage[55] du véhicule *via* une application mobile, etc.) ;
  - **vérifier le kilométrage parcouru** avec le véhicule au cours de la location **afin d'ajuster la facturation,** le cas échéant ;
  - **vérifier l'absence de franchissement de frontières ou d'entrée du véhicule dans des zones de circulation prohibées par les conditions contractuelles** au cours de la location, ce afin d'adapter la facturation, le cas échéant, voire de mettre fin au service.
- **la gestion de la performance du service,** notamment pour **gérer les locations suivantes.** La localisation est, par exemple, utilisée afin d'estimer la durée du retard d'un locataire pour évaluer la nécessité d'acheminer un autre véhicule pour le locataire suivant ;

224. L'utilisation de la donnée de localisation pour la gestion de la flotte ne sera pas toujours la même selon que :

- **les véhicules sont loués par le biais d'une agence de location physique,** à laquelle se rend le client pour récupérer le véhicule (la « location physique ») ; ou que
- **les véhicules sont loués à distance, par le biais d'une borne, d'un site internet ou d'une application, sans intervention physique d'une personne de la société de location** (la « location à distance »). Ce dernier cas vise notamment les hypothèses de location de véhicules en libre-service (on parle notamment d'autopartage ou de *free floating*).

Déterminer les rôles de chaque acteur

225. **La société de location, avec laquelle l'utilisateur du véhicule loué conclut un contrat**, est en principe responsable du traitement pour les finalités relatives à la gestion de l'exécution des contrats de location et à la gestion de la performance du service dès lors que :

- **ces finalités sont déterminées par la société de location** et concernent l'exécution et la gestion du contrat de location et la performance de son service ;
- **la société de location détermine également les moyens essentiels du traitement** : la collecte des données de localisation a généralement lieu *via* un boîtier télématique qu'elle a installé ou fait installer sur le véhicule, ou *via* son application mobile dédiée, permettant la location, ou *via* un capteur GPS dont elle a équipé le véhicule (lorsqu'il s'agit de ses propres véhicules). Les données de localisation sont ensuite traitées en local et/ou remontées vers les serveurs de la société de location ou de son sous-traitant pour y être traitées, selon les modalités qu'elle prévoit.

226. Dans certains cas, et pour certains types de véhicules, les données de localisation sont collectées par le biais de **dispositifs intégrés au véhicule par le constructeur** auxquelles la société de location n'a pas accès (tels que le capteur GPS, directement intégré au système de contrôle du véhicule). Ces données peuvent être **mises à disposition des loueurs par le biais d'une API dédiée**. Dans cette hypothèse, **la société de location reste responsable du traitement pour les finalités** relatives à la gestion commerciale de sa flotte ; le constructeur peut-être, le cas échéant, responsable du traitement de ces données pour les finalités qui lui sont propres.

---

[55] La location à distance implique souvent le déverrouillage et le verrouillage du véhicule sans clef, soit (i) via le téléphone mobile multifonction de l'usager, qui interagit par GSM ou Bluetooth avec un boîtier connecté ; (ii) via une carte RFID fournie par l'opérateur ; (iii) via la carte du réseau de transport public alors lue par un lecteur RFID du boitier connecté. Dans les hypothèses où le déverrouillage et le verrouillage s'effectuent à l'aide du téléphone, des données de localisation sont généralement collectées afin de vérifier que l'utilisateur se trouve bien à proximité du véhicule.

227. Enfin, la société de location peut recourir à des **sous-traitants pour collecter et traiter la donnée de localisation, tels que :**

- les fournisseurs des boîtiers télématiques. Les données de localisation peuvent transiter sur les serveurs de ces derniers avant d'être mis à disposition des sociétés de location ;
- les intégrateurs de données qui jouent le rôle d'intermédiaire entre les constructeurs et les gestionnaires de flotte afin de permettre la mise à disposition des données.

Identifier les bases légales mobilisables

Applicabilité de l'article 82 de la loi Informatique et Libertés

228. La collecte et le traitement des données de localisation des véhicules loués implique d'**accéder à des informations stockées dans un terminal** : accès aux données stockées dans le véhicule connecté, collectées par le constructeur et mises à disposition de la société de location ; accès aux données du boitier télématique dont est équipé le véhicule ou encore accès aux données du téléphone portable de l'utilisateur. L'article 82 de la loi Informatique et Libertés est donc applicable.

229. Le consentement de l'utilisateur n'est toutefois pas requis pour les finalités de gestion de flotte dès lors que l'accès à ces données, et leur traitement, est nécessaire à la fourniture du service de location.

Base légale mobilisable au titre du RGPD

Le tableau ci-après, qui n'a pas vocation à être exhaustif, recense les bases légales pouvant être retenues en fonction de chaque finalité poursuivie par le ou les traitement(s) des données de localisation à des fins de gestion de flotte.

Le responsable du traitement demeure responsable du choix, au cas par cas, de la base légale pour ses traitements de données et devra être en mesure de le justifier.

Le responsable du traitement devra, en tout état de cause, tenir compte de l'obligation d'obtenir le consentement de l'utilisateur pour l'accès aux informations du terminal lorsqu'il est requis par l'article 82 de la loi Informatique et Libertés.

Finalités de la collecte des données de localisation		Mode de location concerné	Base légale mobilisable (si les conditions sont réunies)
Gestion de l'exécution des contrats de location	**Organisation de la fourniture et de la restitution du véhicule**	Location à distance	Contrat
	Vérification de l'absence de franchissement de frontières ou d'entrée du véhicule dans des zones de circulation prohibées par les conditions contractuelles	Location physique ou à distance	Contrat
	Vérification du kilométrage parcouru, en cas de location au kilomètre		Contrat
Gestion de la performance du service	**Identification de la localisation du véhicule pour gérer les éventuels retards à la restitution du véhicule**	Location physique ou à distance	Contrat

Exemple 1

La collecte des données de localisation du véhicule peut reposer sur le contrat lorsque ce traitement est nécessaire à l'exécution du contrat de location, et notamment à la vérification du respect de l'interdiction d'entrer ou de sortir de certaines zones (telles qu'une zone non carrossable ou un autre pays).

Le traitement doit toutefois être limité à ce qui est nécessaire pour l'exécution du contrat : une attention particulière doit donc être portée à la minimisation des données et à la limitation de la durée de conservation de ces données.

Exemple 2

La location de véhicules au kilomètre nécessite la vérification du kilométrage parcouru au cours de la location pour la bonne exécution du contrat, puisque la facturation en dépend.

Le traitement des données de localisation ne peut pas être fondé sur la base légale du contrat lorsqu'il existe des moyens aussi efficaces, et moins intrusifs, pour atteindre la finalité poursuivie. Le traitement des données de l'odomètre (sous réserve que le véhicule en soit équipé) est, généralement, suffisant à cette fin.

Le recours aux données de localisation peut toutefois être nécessaire lorsque le véhicule n'est pas équipé d'odomètre, ou à des fins de contrôle de l'exactitude des données de l'odomètre, afin de comparer ces données à la distance calculée à partir des données de localisation et vérifier ainsi leur cohérence (notamment pour identifier les cas de défaut, ou de manipulation de l'odomètre). Dans ces hypothèses, le responsable du traitement pourrait fonder le traitement des données de localisation sur le contrat dès lors que la vérification du nombre de kilomètres effectivement parcouru avec le véhicule est nécessaire pour facturer le service.

Le traitement doit toutefois être limité à ce qui est nécessaire pour l'exécution du contrat : une attention particulière doit donc être portée à la minimisation des données et à la limitation de la durée de conservation de ces données.

Appliquer les principes de minimisation et de limitation de la conservation des données

Rappel

La CNIL recommande aux acteurs de **privilégier les traitements de données de localisation en local**, au sein du véhicule ou du **dispositif** connecté au véhicule, lorsque cela est pertinent au regard des finalités poursuivies (voir partie 3 relative aux recommandations générales, point 3.6).

Dans les **hypothèses où il est nécessaire de remonter les données de localisation au sein des serveurs** du responsable du traitement, ce dernier doit notamment tenir compte des recommandations relatives au cas d'une base de données servant des finalités multiples (voir point 3.6).

Le tableau ci-après, qui n'a pas vocation à être exhaustif, recense les éléments déclencheurs de l'activation et de la désactivation de la localisation ainsi que les durées de conservation pouvant être retenus en fonction de chaque finalité poursuivie par le ou les traitement(s) des données de localisation à des fins de gestion de flotte.

Le terme « activation » de la localisation peut désigner, selon les cas, le déclenchement de la collecte des données par le dispositif de localisation et/ou la remontée de ces données vers les serveurs de la société de location. Le terme « désactivation » de la localisation désigne, à l'inverse, l'arrêt de la collecte des données et/ou l'arrêt de la remontée de ces données.

Finalités de la collecte des données de localisation		Activation/désactivation de la localisation	Minimisation et durée de conservation des données
Gestion de l'exécution des contrats de location	**Organisation de la fourniture et de la restitution du véhicule**	Activation lorsque l'utilisateur effectue une action positive (par exemple, et selon les cas, pour identifier la localisation d'un véhicule ; pour signaler la fin d'une location ; pour verrouiller ou déverrouiller le véhicule) Désactivation après le démarrage ou le déverrouillage / après la fin de la location ou le verrouillage du véhicule loué.	Selon le cas : • jusqu'au déverrouillage / démarrage ou du véhicule, ; • jusqu'à la restitution du véhicule ; • jusqu'à l'abandon de l'action de l'utilisateur (exemple : fermeture de l'application dédiée après avoir lancé une recherche des véhicules disponibles aux alentours). À la fin de la location, la localisation du véhicule peut toutefois être conservée jusqu'à sa location par une autre personne, afin de pouvoir indiquer son emplacement au locataire suivant.
	Vérification de l'absence de franchissement de frontières ou d'entrée du véhicule dans des zones de circulation prohibées par les conditions contractuelles et ajustement de la facturation	Activation au démarrage du véhicule. Désactivation à l'arrêt du véhicule.	**En l'absence de franchissement de zone prohibée :** La conservation de la dernière position du véhicule est suffisante : chaque donnée de localisation collectée peut écraser la donnée précédente. À la fin de la location, aucune donnée de localisation ne doit être conservée. **En cas de détection d'un franchissement de zone prohibée :** Il est possible de conserver davantage de données. Le responsable de traitement doit néanmoins pouvoir justifier du besoin opérationnel de conservation de ces données.

Finalités de la collecte des données de localisation		Activation/désactivation de la localisation	Minimisation et durée de conservation des données
	Vérification du kilométrage pour ajuster la facturation	Activation au démarrage du véhicule. Désactivation à l'arrêt du véhicule.	**Jusqu'à la conversion des positions en distance**. *Les données de localisation n'ont pas vocation à être conservées une fois qu'elles ont été traitées pour calculer la distance parcourue : les données de localisation peuvent être automatiquement converties en distance (calcul sur la base des positions du véhicule) et être supprimés, au fur et à mesure qu'elles sont remplacées par de nouvelles données (conservation uniquement des données de distances, additionnées au fur et à mesure pour déterminer le nombre de kilomètres parcourus avec le véhicule au cours de la location).* **La conservation des données de localisation n'est, en tout état de cause, pas nécessaire pour cette finalité une fois la location terminée.**
Gestion de de la performance du service	**Identification de la localisation du véhicule pour gérer les éventuels retards à la restitution du véhicule**	Activation avant l'horaire de restitution du véhicule. *Il appartient au responsable du traitement de déterminer la durée nécessaire, avant l'horaire de restitution du véhicule, pour qu'il puisse assurer la gestion du retard.* *La collecte de la donnée de localisation tout au long du trajet ne semble toutefois pas nécessaire.* Désactivation à la restitution du véhicule.	**Jusqu'à la restitution du véhicule.** *Il semble suffisant que seule la dernière position soit conservée.* **La conservation des données de localisation n'est, en tout état de cause, pas nécessaire pour cette finalité une fois la location terminée.**

Exemple

Une société de location traite les données de localisation des véhicules loués afin de vérifier que ses clients ne violent pas l'interdiction d'entrer ou de sortir de certaines zones (telles qu'une zone non carrossable ou un autre pays) prévues par le contrat de location. Ce traitement peut être effectué afin d'être en mesure d'adapter la facturation, le cas échéant.

Dans cette hypothèse, la conservation d'un historique complet du trajet n'est pas nécessaire et ne serait donc pas conforme au principe de minimisation des données.

Pour atteindre la finalité poursuivie, et respecter les conditions de mobilisation de l'intérêt légitime, la CNIL recommande :

- une collecte des données de localisation de manière peu fréquente (espacée). Cette fréquence doit être déterminée en fonction de la zone géographique concernée : si seule la circulation dans un autre Etat est interdite, la granularité des données de localisation nécessaire est moins fine que dans l'hypothèse où l'interdiction porte sur des zones non carrossables.
- un écrasement de chaque donnée par la nouvelle position collectée, sauf en cas d'identification de l'entrée du véhicule dans une zone interdite (mécanisme similaire au géorepérage[56]). La conservation de positions espacées semble généralement suffisante une fois le franchissement identifié, sans qu'il soit nécessaire pour le responsable du traitement de connaitre le trajet continu effectué dans la zone concernée.

230. Les données de localisation du véhicule **peuvent toutefois être conservées** au-delà des durées indiquées dans le tableau en **cas de suspicion de vol** (voir les recommandations spécifiques à cette finalité au point 5.1) **ou à des fins d'établissement de preuves** dans certains cas exceptionnels où le responsable de traitement identifie un risque contentieux, selon une analyse au cas par cas et dument documentée[57].

Garantir l'information et l'exercice des droits des personnes concernées

231. Les sociétés de location sont tenues de respecter les obligations d'information des personnes concernées sur les traitements de données de localisation qu'elles effectuent.

232. Pour se conformer à ces obligations, une bonne pratique est de mettre en œuvre différentes modalités d'information combinées.

233. En effet, **le client doit recevoir, au moment de la souscription au service de location, une information dédiée**. Cette information peut se trouver au sein du contrat de location ou dans une politique de confidentialité dédiée, et être délivrée soit par voie dématérialisée, soit au format papier, selon le mode de souscription.

234. A titre de bonnes pratiques, la CNIL encourage le recours, de manière complémentaire, à d'autres modalités d'informations afin d'assurer la transparence des traitements de données, y compris à l'égard des personnes qui ne sont pas partie au contrat avec la société (tels que les autres conducteurs ou les éventuels passagers)[58].

[56] Le géorepérage, ou « geofencing » en anglais, désigne généralement une technique qui s'appuie sur les technologies de localisation qui permet de surveiller/suivre les déplacements d'objets ou de personnes dans un périmètre défini.

[57] Dans cette hypothèse, la conservation des données de localisation poursuivrait une autre finalité, pour laquelle l'ensemble des obligations prévues par le RGPD devront également être respectées (base légale, information, etc.). La durée de conservation des données à des fins probatoires pourra, au maximum, correspondre aux durées de prescriptions légales applicables. Pendant cette durée, les données doivent faire l'objet d'un archivage intermédiaire, puisqu'elles ne sont plus utilisées pour la finalité courante pour laquelle elles ont été collectées, et devront être supprimée dès que leur conservation n'est plus nécessaire (résolution du litige, issue de la procédure judiciaire, etc.).

[58] Voir en ce sens le point 3.7 de la recommandation.

L'usage de la localisation à des fins d'assistance aux personnes et de dépannage du véhicule loué en cas de panne ou d'accident[59]

235. Les données de localisation peuvent s'avérer utiles en cas de panne, de dysfonctionnement ou d'accident du véhicule : elles permettent d'identifier avec précision le lieu où le véhicule loué se trouve, facilitant ainsi la prise en charge par une société en charge de la prestation d'assistance.

Déterminer les rôles de chaque acteur

236. La prestation d'assistance peut être prise en charge directement par le gestionnaire de flotte (prestation internalisée) ou être externalisée auprès d'une société en charge de la prestation d'assistance.

Cas 1 : la prestation d'assistance est opérée directement par le gestionnaire de flotte.

237. Le gestionnaire de flotte est le responsable du traitement dès lors :

- qu'il décide de traiter les données, notamment les données de localisation, afin de permettre l'exécution de la prestation d'assistance ;
- qu'il détermine les moyens du traitement et notamment les données collectées, les moyens techniques utilisés pour collecter ces données, la fréquence de la collecte ainsi que la durée de conservation.

Cas 2 : la prestation d'assistance est opérée par une société, distincte du gestionnaire de flotte.

238. Le gestionnaire de flotte peut faire le choix d'externaliser la prestation d'assistance en la confiant à une société tierce qui sera destinataire des données de localisation. La situation doit alors faire l'objet d'une analyse au cas par cas.

239. Au regard de la pratique sectorielle, les données de localisation sont, en principe, collectées par le gestionnaire de flotte puis transmises à la société en charge de la prestation d'assistance avec laquelle il entretient une relation contractuelle, en cas de besoin.

240. Le gestionnaire de flotte et la société en charge de la prestation d'assistance pourront être considérés comme responsables conjoints du traitement s'ils ont décidé ensemble de traiter les données de localisation afin de permettre l'exécution de la prestation d'assistance et déterminé les moyens essentiels du traitement notamment le moment et la fréquence de la collecte, les modalités de transmission des données ainsi que la durée de conservation.

241. Dans ce cas, chaque responsable du traitement doit évaluer l'étendue de son niveau de responsabilité, les acteurs n'étant pas nécessairement responsables des mêmes opérations du traitement. En effet, leur responsabilité peut varier en fonction de leur implication sur les opérations du traitement pour la finalité définie en commun.

242. À défaut, le gestionnaire de flotte peut être considéré comme un sous-traitant s'il agit au nom et pour le compte de la société en charge de la prestation d'assistance.

Exemple

Dans le cadre d'un service de location de scooters électriques, le loueur propose un service d'assistance au dépannage dans le contrat.

Le loueur et la société en charge de la prestation d'assistance décident conjointement de traiter les données de localisation afin de permettre l'exécution d'une prestation d'assistance en cas de panne ou d'accident. Le loueur peut décider des modalités de collecte (moment, fréquence) et de transmission de la donnée de localisation. La société en charge de la prestation d'assistance détermine pour sa part, la façon dont elle récupère et exploite la donnée de localisation auprès du loueur et la durée de conservation des données de géolocalisation.

[59] A la différence de système eCall embarqué fondé sur le numéro 112, il s'agit ici de situations non urgentes ne nécessitant pas l'intervention des services de secours.

Identifier les bases légales mobilisables

Applicabilité de l'article 82 de la loi Informatique et Libertés

243. Pour collecter et traiter les données de localisation, le gestionnaire de flotte est amené à **accéder à des informations stockées dans un terminal** : accès aux données du boitier télématique dont est équipé le véhicule.

244. L'accès à ces informations **nécessite donc le consentement de l'utilisateur** (le client, locataire du véhicule) sauf lorsque cet accès est nécessaire à la fourniture du service expressément demandé par l'utilisateur.

245. En ce qui concerne l'accès aux données de localisation à des fins d'assistance aux personnes et de dépannage du véhicule en cas de panne ou d'accident :

- Soit ce service fait l'objet d'une clause contractuelle ad hoc, optionnelle, ou d'un contrat spécifique et les données sont alors nécessaires à ce service spécifique, souscrit par le client ; un consentement, au titre de l'article 82 de la loi Informatique et libertés n'est pas requis ;
- Soit ce service est automatiquement associé par le responsable du traitement à la location du véhicule ; dans ce cas, le traitement ne peut être regardé comme nécessaire au service de location de véhicule qui est demandé par l'utilisateur car il en constitue un accessoire détachable ; un consentement est requis au titre de l'article 82 de la loi Informatique et Libertés et, s'il est refusé, le service ne doit pas être activé.

Bases légales mobilisables au titre du RGPD

246. Le responsable du traitement demeure responsable du choix, au cas par cas, de la base légale pour ses traitements de données et devra être en mesure de le justifier.

247. Si l'assistance constitue une prestation optionnelle entre le gestionnaire de flotte et le client alors la base légale du contrat (article 6.1.b du RGPD) peut être mobilisée pour le traitement des données de localisation à cette fin.

Point d'attention

Si la prestation d'assistance fait partie des prestations de base incluses dans le contrat de location souscrit par le client sans que le client n'ait la possibilité de la refuser, l'exécution du contrat ne constitue pas une base juridique pertinente pour le traitement des données de localisation, l'objectif principal du contrat étant de fournir un service de location au client final. Si le traitement des données de localisation est utile à la poursuite de la finalité d'assistance et de dépannage, il n'apparaît pas nécessaire à l'objet même du contrat conclu entre le gestionnaire de flotte et le client, la location du véhicule pouvant être effectuée sans que ce traitement soit mis en œuvre.

Dans cette hypothèse, le gestionnaire de la flotte peut se fonder sur le consentement (article 6.1.a du RGPD) pour le traitement des données de localisation pour la finalité de d'assistance aux personnes et de dépannage du véhicule, dès lors que ce consentement devra être recueilli au titre de l'article 82 de la loi « Informatique et libertés ». Les deux consentements peuvent être recueillis ensemble.

Appliquer les principes de minimisation et de limitation de la conservation des données

La minimisation des données collectées

248. Le responsable du traitement doit déterminer la granularité et la fréquence de la collecte.

249. La CNIL recommande de collecter et de remonter la localisation du véhicule au moment où l'utilisateur opère sa demande de prise en charge.

250. En effet, la localisation du véhicule ne semble pas nécessaire avant la survenance de la panne ou de l'accident, dont l'utilisateur sera en mesure d'informer le service d'assistance. Il appartient aux responsables du traitement de démontrer, au cas par cas, la nécessité de collecter les données de localisation ainsi que celle de les remonter sur des serveurs distants avant toute demande de prise en charge de l'utilisateur.

251. Parfois le gestionnaire de flotte a déjà collecté les données de localisation du véhicule pour différentes finalités et les a remontées sur ses serveurs. Dans cette situation, l'accès à la localisation du véhicule à des fins d'assistance en cas de panne ou d'accident ou le cas échéant, sa transmission à la société en charge de la

prestation d'assistance, est conditionné à la demande de prise en charge de l'utilisateur, constitutive du fait générateur. Dès lors que seule la dernière position apparaît nécessaire au regard de la finalité, la CNIL recommande que seule cette dernière position soit accessible ou transmise.

La limitation de la conservation des données

252. Si des données de localisation des véhicules peuvent être nécessaires à l'accomplissement d'un service d'assistance et de dépannage à l'utilisateur victime d'une panne ou d'un accident, elles ne le sont plus dès lors que ce service ou les procédures qui y sont liées prennent fin. Sauf disposition légale spécifique, les données de localisation doivent alors être supprimées.

Garantir l'information des personnes concernées

253. Le responsable du traitement est tenu de respecter les obligations d'information des personnes concernées sur les traitements de données de localisation qu'il effectue.

254. En effet, le client doit recevoir, au moment de la souscription au service de location, une information dédiée. Cette information peut se trouver au sein du contrat de location ou dans une politique de confidentialité dédiée, et être délivrée soit par voie dématérialisée, soit au format papier, selon le mode de souscription.

255. La CNIL recommande que l'information se fasse au moment de la signature du contrat incluant la prestation de dépannage. En tout état de cause, l'information doit être délivrée avant la collecte des données de localisation à cette fin.

256. Lorsque la prestation d'assistance est opérée par une société en charge de la prestation d'assistance distincte du gestionnaire de flotte, l'usager du service doit être informé que les données de localisation collectées par le gestionnaire de flotte sont transmises à la société en charge de la prestation d'assistance afin de permettre l'exécution de la prestation d'assistance.

257. En présence de responsables conjoints du traitement, l'accord qui les lie doit prévoir leurs obligations respectives quant à la communication aux usagers du service, des informations visées aux articles 13 et 14 du RGPD.

6. FOCUS - Technologies de localisation : boîtiers télématiques et agrégateurs de données

- Les **boîtiers télématiques :**

258. Les **boîtiers télématiques**, initialement conçus pour des applications professionnelles telles que la gestion de flotte professionnelle, la maintenance des véhicules et les besoins en logistique, peuvent également être **présents dans les flottes de véhicules destinées à des clients particuliers**.

259. Les données de localisation remontées par ces boîtiers peuvent, par exemple, être utiles pour **retrouver un véhicule** appartenant à un gestionnaire de flotte ou à un particulier, ainsi que pour savoir quand effectuer la **réparation d'un véhicule** de manière préventive par exemple, en fonction du kilométrage.

- Les **agrégateurs de données :**

260. Les **agrégateurs de données** se fondent quant à eux sur les données remontées par les **API des constructeurs de véhicules**. Ces API remontent des données provenant des capteurs internes d'un véhicule [60], dont les données de localisation. Les agrégateurs de données fournissent ainsi une solution permettant de collecter ces données et d'offrir une **vision harmonisée des données** d'une flotte de véhicules, même si des **API de constructeurs différents** sont à l'origine des données collectées.

261. De **façon similaire aux boîtiers télématiques**, les données remontées peuvent servir pour la localisation d'un véhicule.

Agrégation de données et agrégateur de données

Le terme « **agrégateur** » employé ci-dessus a une signification différente de la technique d'**agrégation** employée lors de l'anonymisation de données, où les données à anonymiser font par exemple l'objet d'une addition ou une moyenne afin de les généraliser.

Les agrégateurs de données fournissent des solutions permettant de consulter et visualiser des données en provenance d'un grand nombre de véhicules. Mais ces données peuvent ne pas être anonymisées.

6.1 Identifier les rôles des acteurs, au cas par cas

262. Selon les cas, les fournisseurs de boîtiers télématiques ou les agrégateurs peuvent être sous-traitants, ou responsables du traitement pour les traitements de données personnelles qu'ils effectuent dans le cadre du service qu'ils proposent :

- Ils sont **sous-traitants** de leurs clients lorsque les données personnelles sont collectées (soit via le boîtier télématique fourni, soit via l'API du constructeur automobile) pour le compte, et sous les instructions de leurs clients.
- Ils sont **responsables du traitement,** lorsqu'ils décident de l'objectif et des modalités de leur traitement (les données collectées, leur durée de conservation, les mesures de sécurité mises en place, etc.).

263. Ils seront, en tout état de cause, responsables du traitement de ces données lorsqu'ils poursuivent des finalités qui leurs sont propres, par exemple, lorsqu'ils traitent les données pour l'amélioration et l'optimisation de leurs services (voir la recommandation spécifique à cette finalité au point 5.3).

264. Chaque acteur **doit déterminer, au cas par cas, sa qualification au regard de son rôle effectif pour chaque traitement de données personnelles** (voir point 3.3). En cas de sous-traitance, le contrat conclu avec le client doit faire état des obligations qui incombent respectivement à chacune des parties en matière de protection des données (article 28 du RGPD), notamment en matière de sécurité.

[60] Lorsqu'une application mobile est fournie par le constructeur, ces API sont souvent utilisées pour afficher les informations provenant du véhicule (consommation, localisation, etc.)

6.2 Recommandations communes

Mettre en œuvre des mesures de sécurité

265. Quelle que soit leur qualification, le fournisseur de boîtier télématique et/ou l'agrégateur de données devront mettre en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque, conformément à l'article 32 du RGPD.

266. Outre les mesures de sécurité générales (voir point 3.9), certaines bonnes pratiques peuvent être mises en œuvre par ces catégories spécifiques d'acteurs.

API et échange de données

267. La CNIL a publié une recommandation concernant les **recommandations et bonnes pratiques** à adopter pour partager des données personnelles par le biais des **API**[61]. Cette recommandation distingue trois rôles (détenteurs de données, gestionnaires d'API et réutilisateurs) qui peuvent être tenus par le même organisme. Par exemple, les constructeurs de véhicules peuvent être considérés comme détenteurs de données et gestionnaires d'API lorsqu'ils mettent à disposition leur API aux agrégateurs de données.

268. Les recommandations et bonnes pratiques contenues dans cette recommandation, notamment sur la sécurité, la minimisation et la sécurité des données, sont également applicables aux API fournies par les constructeurs des véhicules ou par les différents acteurs fournissant des API transmettant des données de localisation.

Cloisonnement des données

269. Les services d'informatique en nuage (services *cloud*) associés aux données transmises par les boitiers télématiques ou aux solutions fournies par les agrégateurs devraient être conçus de manière à **séparer les données des différents clients.** L'utilisation de plusieurs **bases de données distinctes** est une bonne pratique pour amoindrir les risques que les données d'un client puissent être accédées frauduleusement ou de manière accidentelle lors de l'accès aux données d'un autre client.

270. Si le numéro d'identification du véhicule (VIN) est collecté, il devrait être protégé par des techniques de hachage cryptographique à l'état de l'art lorsque ce numéro n'est pas utile au traitement[62].

6.3 Recommandations spécifiques concernant la sécurité des boîtiers télématiques

271. En plus des recommandations générales, quelques recommandations spécifiques sont également applicables aux fournisseurs de boitiers télématiques.

Chiffrement des données au repos et en transit

272. La CNIL recommande de mettre en place des **mécanismes de chiffrement robustes** pour protéger les données **stockées et transmises**. Le chiffrement de la mémoire flash est par exemple une mesure adéquate pour s'assurer que les données de localisation ne puissent pas être lues en cas de vol ou de perte du boîtier.

273. Les boîtiers télématiques utilisent généralement une puce 4G ou 5G pour la connectivité, bien que certains boitiers permettent également l'utilisation du Wi-Fi lorsque cela est possible. La communication entre le boîtier et les serveurs associés devrait être sécurisée par des **protocoles cryptographiques à l'état de l'art**, tels que TLS, ou par l'utilisation de liaison VPN pour une sécurité accrue.

274. Concernant le chiffrement au repos des données, la CNIL recommande un **chiffrement de la mémoire flash** contenant les données de localisation.

---

[61] Recommandation technique relative à l'utilisation des interfaces de programmation applicatives (API) pour le partage sécurisé de données à caractère personnel, 2023. URL : https://www.cnil.fr/sites/cnil/files/2023-07/recommandation_api.pdf

[62] Voir également la point 3.10. « Appliquer les mesures de protection des données dès la conception » dans les recommandations générales.

Stockage des données

275. La CNIL recommande d'utiliser les capacités de calcul locales du véhicule ou du boitier, pour effectuer le plus en amont possible les traitements relatifs aux données de localisation. Par exemple, si les données sont disponibles, des traitements de généralisation des données peuvent être effectués dès leur réception par le véhicule ou le boitier, au lieu de les effectuer dans des serveurs distants.

276. L'espace de stockage des boîtiers télématiques est souvent limité, **ce qui rend également préférable une minimisation des données collectées dès leur réception** : les nouvelles données remplaçant généralement les anciennes.

Contrôle et désactivation à distance

277. La CNIL recommande que les boîtiers télématiques soient conçus pour être **désactivables à distance. Cette fonctionnalité est essentielle pour permettre directement au gestionnaire de flotte ou indirectement au conducteur de contrôler l'activation et la désactivation du service**, conformément aux principes de protection des données par défaut et par conception. Cette possibilité de désactivation devrait être possible à tout moment.

Sécurité physique et logique

278. Les fournisseurs devraient également être attentifs aux **moyens physiques d'accéder aux informations** contenues dans les boitiers, par exemple aux connecteurs servant au débogage[63] sur les cartes électroniques, qui peuvent être utilisés pour accéder directement à la mémoire du boîtier. Des mesures de sécurité physique et logique devraient être mises en place pour protéger ces points d'accès et empêcher tout accès non autorisé aux données sensibles.

279. La CNIL recommande ainsi la désactivation matérielle des interfaces de débogage dans les systèmes embarqués. Des procédures de démarrage sécurisé ainsi que des moyens physiques d'empêcher un accès aux mémoires/supports de stockage devraient également être mis en œuvre dans ces systèmes.

6.4 Recommandations spécifiques concernant la sécurité des solutions fournies par les agrégateurs de données de localisation

280. En plus des recommandations générales, quelques recommandations spécifiques sont également applicables aux agrégateurs de données de localisation.

Contrôle et désactivation à distance

281. Les solutions d'agrégation devraient être conçues de manière à pouvoir **désactiver la remontée de la localisation à distance vers le gestionnaire de flotte si les données de localisation ne sont pas nécessaires au service.**

282. Cette fonctionnalité est de même essentielle pour permettre directement au gestionnaire de flotte ou indirectement au conducteur de contrôler l'activation et la désactivation du service, conformément aux principes de protection des données par défaut et par conception. Cette possibilité de désactivation devrait être possible à tout moment.

Mode de mise à disposition des données

283. À titre de bonne pratique, les agrégateurs peuvent concevoir leur solution de sorte à permettre aux utilisateurs des données de ne collecter que les données qui leurs sont nécessaires, afin de faciliter le respect par ces derniers du principe de minimisation.

284. À cet égard, différentes modalités peuvent être envisagées, à l'instar d'API sécurisées disposant d'un degré de granularité suffisamment fin ou, en permettant aux utilisateurs des données un paramétrage fin des données auxquelles ils accèdent ou qu'ils téléchargent. Il apparaît également pertinent à cette fin de proposer, pour un même client, la possibilité de créer de plusieurs profils disposant de droits d'accès distincts aux données.

[63] Tels que les connecteurs JTAG ou série.