

Commission nationale de l'informatique et des libertés

Délibération n° 2015-165 du 4 juin 2015 portant adoption d'une norme simplifiée concernant les traitements automatisés de données à caractère personnel mis en œuvre par les organismes publics ou privés destinés à géolocaliser les véhicules utilisés par leurs employés (norme simplifiée n° 51)

NOR : CNIL1513960X

La Commission nationale de l'informatique et des libertés,

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

Vu le règlement (CEE) n° 3821/85 modifié du 20 décembre 1985 concernant l'appareil de contrôle installé et utilisé sur les véhicules affectés aux transports par route de voyageurs ou de marchandises soumis aux dispositions du règlement (CEE) n° 3820/85 du 20 décembre 1985 relatif à l'harmonisation de certaines dispositions en matière sociale dans le domaine des transports par route ;

Vu la directive 95/47/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données ;

Vu la directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement de données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques ;

Vu la recommandation du Conseil de l'Europe du 1^{er} avril 2015 sur le traitement des données à caractère personnel dans le cadre de l'emploi ;

Vu le code du travail ;

Vu le code de la route ;

Vu la loi du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, notamment le I de son article 24 ;

Vu les lois n° 83-634 du 13 juillet 1983 portant droits et obligations des fonctionnaires, n° 84-16 du 11 janvier 1984 portant dispositions statutaires relatives à la fonction publique de l'Etat, n° 84-53 du 26 janvier 1984 portant dispositions statutaires relatives à la fonction publique territoriale, et n° 86-33 du 9 janvier 1986 portant dispositions statutaires à la fonction publique hospitalière ;

Vu le décret n° 2005-1309 du 20 octobre 2005 pris pour l'application de la loi du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés ;

Vu les avis du groupe de travail dit de l'« article 29 » en date 13 septembre 2001 sur le traitement de données à caractère personnel dans le contexte professionnel et du 25 novembre 2005 sur l'utilisation de la donnée de géolocalisation en vue de fournir un service à valeur ajoutée ;

Vu la délibération de la Commission nationale de l'informatique et des libertés n° 2006-067 du 16 mars 2006 portant adoption d'une norme simplifiée concernant les traitements automatisés de données à caractère personnel mis en œuvre par les organismes publics ou privés destinés à géolocaliser les véhicules utilisés par leurs employés ;

Après avoir entendu Mme Marie-France Mazars, commissaire, en son rapport, et M. Jean-Alexandre SILVY, commissaire du Gouvernement, en ses observations ;

Formule les observations suivantes :

En vertu de l'article 24 de la loi du 6 janvier 1978 modifiée, la Commission nationale de l'informatique et des libertés est habilitée à établir des normes destinées à simplifier l'obligation de déclaration des traitements les plus courants et dont la mise en œuvre, dans des conditions régulières, n'est pas susceptible de porter atteinte à la vie privée ou aux libertés.

La Commission nationale de l'informatique et des libertés constate le développement de dispositifs dits de géolocalisation permettant aux organismes privés ou publics de prendre connaissance de la position géographique, à un instant donné ou en continu, des employés par la localisation des véhicules mis à leur disposition pour l'accomplissement de leur mission.

Ces traitements sont à distinguer des traitements issus de la mise en œuvre des appareils de contrôle dans le domaine du transport par route (chronotachygraphes), ces derniers bénéficiant quant à eux d'une dispense de déclaration en application de la délibération de la commission n° 2014-235 du 27 mai 2014.

L'information relative à la géolocalisation d'un employé peut être directement issue d'un logiciel installé au sein de l'organisme privé ou public ou accessible par l'intermédiaire d'un site web d'un prestataire de service.

Ces traitements, en ce qu'ils permettent de collecter la donnée relative à la localisation du véhicule dont un employé déterminé a l'usage et d'identifier ainsi les déplacements de cet employé, portent sur des données à caractère personnel et sont soumis aux dispositions de la loi du 6 janvier 1978 modifiée, notamment celles relatives aux formalités préalables.

La commission a adopté, le 16 mars 2006, une norme permettant de simplifier la déclaration des traitements visant à géolocaliser un véhicule utilisé par un employé. Compte tenu de l'évolution des pratiques, il lui est apparu nécessaire de compléter cette norme.

Décide :

Art. 1^{er}. – Seuls peuvent bénéficier de la procédure de la déclaration simplifiée de conformité à la présente norme les traitements automatisés relatifs à la géolocalisation des véhicules utilisés par les employés d'organismes publics ou privés qui répondent aux conditions définies aux articles suivants.

Art. 2. – *Finalités du traitement.*

A titre liminaire, la commission rappelle que des données à caractère personnel ne peuvent être collectées que pour des finalités déterminées, explicites et légitimes et qu'elles ne doivent pas être traitées ultérieurement de manière incompatible avec ces finalités.

Les traitements couverts par la présente norme ne peuvent être mis en œuvre que pour tout ou partie des finalités suivantes :

a) Le respect d'une obligation légale ou réglementaire imposant la mise en œuvre d'un dispositif de géolocalisation en raison du type de transport ou de la nature des biens transportés ;

b) Le suivi et la facturation d'une prestation de transport de personnes ou de marchandises ou d'une prestation de services directement liée à l'utilisation du véhicule, ainsi que la justification d'une prestation auprès d'un client ou d'un donneur d'ordre ;

c) La sûreté ou la sécurité de l'employé lui-même ou des marchandises ou véhicules dont il a la charge, en particulier la lutte contre le vol du véhicule ;

d) Une meilleure allocation des moyens pour des prestations à accomplir en des lieux dispersés, notamment pour des interventions d'urgence ;

e) Le contrôle du respect des règles d'utilisation du véhicule définies par le responsable de traitement, sous réserve de ne pas collecter une donnée de localisation en dehors du temps de travail du conducteur.

Le traitement peut avoir pour finalité accessoire le suivi du temps de travail, lorsque ce suivi ne peut être réalisé par un autre moyen, sous réserve notamment de ne pas collecter ou traiter de données de localisation en dehors du temps de travail des employés concernés.

Art. 3. – *Données traitées.*

La commission rappelle que des données à caractère personnel ne peuvent être collectées que si elles sont adéquates, pertinentes et non excessives au regard de la finalité poursuivie par le responsable de traitement. Ce dernier doit ainsi être en mesure de justifier du caractère nécessaire des données à caractère personnel effectivement collectées.

Pour atteindre les finalités mentionnées à l'article 2 de la présente norme, un responsable de traitement peut collecter et traiter :

a) L'identification de l'employé : nom, prénom, coordonnées professionnelles, matricule interne, numéro de plaque d'immatriculation du véhicule ;

b) Les données relatives aux déplacements des employés : données de localisation issues de l'utilisation d'un dispositif de géolocalisation, historique des déplacements effectués ;

c) Les données complémentaires associées à l'utilisation du véhicule : vitesse de circulation du véhicule, nombre de kilomètres parcourus, durées d'utilisation du véhicule, temps de conduite, nombre d'arrêts ;

d) La date et l'heure d'une activation et d'une désactivation du dispositif de géolocalisation pendant le temps de travail.

Sauf si une disposition légale le permet, le traitement de la vitesse maximale ne peut s'effectuer, conformément à l'article 9 de la loi qui interdit notamment aux personnes privées de mettre en œuvre des traitements visant à faire directement apparaître des données relatives aux infractions.

Par ailleurs, pour ne pas porter atteinte au respect de l'intimité de la vie privée, il n'est pas possible de collecter une donnée de localisation en dehors du temps de travail du conducteur, en particulier lors des trajets effectués entre son domicile et son lieu de travail ou pendant ses temps de pause.

Art. 4. – *Destinataires des données.*

La commission rappelle que le responsable d'un traitement de données à caractère personnel est tenu, en application de l'article 34 de la loi du 6 janvier 1978 modifiée, de prendre toutes les garanties utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données, notamment, empêcher que des tiers non autorisés y aient accès.

A ce titre, le responsable d'un traitement, avant de transmettre des données à un organisme, doit opérer un tri parmi ces dernières pour veiller à ce que le destinataire accède aux seules données adéquates, pertinentes et non excessives au regard de la justification de la communication.

Seuls les employés habilités du responsable de traitement, dans la limite de leurs attributions respectives, doivent pouvoir accéder aux données à caractère personnel traitées dans le cadre d'un dispositif de géolocalisation, en particulier les personnes en charge de coordonner, de planifier ou de suivre les interventions, les personnes en charge de la sécurité des biens transportés ou des personnes ou, le cas échéant, le responsable des ressources humaines.

Pour rendre compte à un client ou à donneur d'ordre sur l'état d'avancement d'une prestation, ou pour justifier de sa réalisation *a posteriori*, le responsable du traitement doit communiquer les seules données nécessaires au regard de cette finalité. L'identité du conducteur du véhicule, sauf à ce qu'elle présente un intérêt particulier dans ce cadre, ne doit pas être communiquée au tiers.

En toutes hypothèses, les données transmises par le responsable de traitement doivent uniquement être rendues accessibles aux personnes habilitées à en connaître au regard de leurs attributions.

Art. 5. – Durée de conservation.

La commission rappelle que des données à caractère personnel doivent être adéquates, pertinentes et non excessives au regard de la finalité pour laquelle elles ont été collectées, d'une part, et qu'elles doivent également être exactes, complètes et si nécessaires mises à jour, d'autre part.

Les données relatives à la localisation d'un employé ne peuvent ainsi être conservées que pour une durée pertinente au regard de la finalité du traitement qui a justifié la collecte.

Au regard des finalités pouvant justifier la mise en place d'un dispositif de géolocalisation telles que prévues à l'article 2 de la présente norme, une durée de deux mois est considérée comme adéquate.

Les données de localisation peuvent être conservées pour une période supérieure à deux mois :

- si une disposition légale le prévoit ;
- si une telle conservation est rendue nécessaire à des fins de preuve de l'exécution d'une prestation, lorsqu'il n'est pas possible de rapporter cette preuve par un autre moyen. Dans ce cas, la durée de conservation est fixée à un an, cette durée ne faisant pas obstacle à une conservation supérieure en cas de contestation des prestations effectuées ;
- si la conservation est effectuée pour conserver un historique des déplacements à des fins d'optimisation des tournées, pour une durée maximale d'un an.

Dans le cadre de la finalité accessoire du suivi du temps de travail, qui implique que ce suivi ne puisse être assuré par un autre moyen, seules les données relatives aux horaires effectués peuvent être conservées pendant une durée de cinq ans.

La commission rappelle qu'il est possible d'archiver des données à caractère personnel, à condition de respecter les dispositions de la délibération de la commission n° 2005-213 du 11 octobre 2005 portant adoption d'une recommandation concernant les modalités d'archivage électronique de données à caractère personnel.

Art. 6. – Information et droits des personnes.

Le responsable du traitement doit procéder, conformément aux dispositions du code du travail et à la législation applicable aux trois fonctions publiques, à l'information et à la consultation des instances représentatives du personnel avant la mise en œuvre d'un dispositif de géolocalisation des employés.

Conformément à l'article 32 de la loi du 6 janvier 1978 modifiée, les employés concernés doivent être informés, préalablement à la mise en œuvre du traitement, de l'identité du responsable de traitement ou de son représentant, de la finalité poursuivie par le traitement, des destinataires ou catégories de destinataires des données, de l'existence d'un droit d'accès aux données les concernant, d'un droit de rectification et d'un droit d'opposition pour motif légitime, ainsi que des modalités d'exercice de ces droits tel que prévu par l'article 90 du décret du 20 octobre 2005.

Les employés doivent avoir la possibilité de désactiver la fonction de géolocalisation des véhicules, en particulier à l'issue de leur temps de travail ou pendant leurs temps de pause, le responsable de traitement pouvant, le cas échéant, demander des explications en cas de désactivations trop fréquentes ou trop longues du dispositif.

Les employés investis d'un mandat électif ou syndical ne doivent en aucun cas faire l'objet d'une opération de géolocalisation lorsqu'ils agissent dans le cadre de l'exercice de leur mandat.

Art. 7. – Mesures de sécurité.

Le responsable du traitement doit prendre toutes les précautions utiles au regard des risques présentés par son traitement pour préserver la sécurité des données à caractère personnel visées à l'article 3 et, notamment au moment de leur collecte, durant leur transmission et leur conservation, empêcher qu'elles soient déformées, endommagées ou que des tiers non autorisés y aient accès.

Pour atteindre cet objectif, le responsable de traitement peut en particulier réaliser une étude des risques liés à la sécurité des données permettant de définir les mesures les plus adaptées au contexte en présence.

En toutes hypothèses, les accès individuels aux données doivent s'effectuer par un identifiant et un mot de passe individuels respectant les recommandations de la commission et régulièrement renouvelé, ou par tout autre moyen d'authentification garantissant au moins le même niveau de sécurité.

Par ailleurs, un mécanisme de gestion des habilitations, régulièrement mis à jour, doit être mis en œuvre pour garantir que les personnes habilitées n'ont accès qu'aux seules données effectivement nécessaires à la réalisation de leurs missions. Le responsable de traitement doit définir et formaliser une procédure permettant de garantir la bonne mise à jour des habilitations.

Toute transmission d'information via un canal de communication non sécurisé, par exemple Internet, doit s'accompagner de mesures adéquates permettant de garantir la confidentialité des données échangées, telles qu'un chiffrement des données. Les moyens utilisés doivent être conformes à l'état de l'art et, le cas échéant, respecter les recommandations de la commission.

Les accès à l'application doivent faire l'objet d'une traçabilité, dont l'intégrité est assurée, afin de permettre la détection d'éventuelles tentatives d'accès frauduleux ou illégitimes, en incluant un horodatage, l'identifiant de l'utilisateur, ainsi que l'identification des données concernées, et ceci pour les accès en consultation, modification ou suppression. Les données de journalisation doivent être conservées pendant une durée de six mois et faire l'objet d'une revue régulière visant à identifier tout incident de sécurité.

La commission rappelle que l'usage d'outils ou de logiciels développés par des tiers dans le cadre de la mise en œuvre d'un traitement de données à caractère personnel reste sous la responsabilité du responsable de traitement, qui doit notamment vérifier que ces outils ou logiciels respectent les obligations que la loi du 6 janvier 1978 modifiée met à sa charge.

La commission rappelle, en cas de recours aux services d'un sous-traitant, que ce dernier ne peut agir que sur instruction du responsable de traitement, lequel n'est pas dispensé de son obligation de veiller au respect des mesures de sécurité qui lui sont imposées par l'article 34 de la loi du 6 janvier 1978 modifiée. Le sous-traitant doit par ailleurs présenter des garanties suffisantes pour assurer la mise en œuvre des mesures de sécurité, et le contrat établi entre les parties doit comporter l'indication des obligations incombant au sous-traitant en matière de sécurité des données à caractère personnel.

La commission rappelle enfin que l'obligation de veiller à la sécurité des données à caractère personnel nécessite la mise à jour des mesures de sécurité au regard de la réévaluation régulière des risques.

Art. 8. – *Mesures transitoires.*

Les organismes privés et publics ayant effectué une déclaration simplifiée en référence à la norme simplifiée n° 51 (délibération n° 2006-067 du 16 mars 2006) qui ne respectent pas les conditions fixées par la présente, disposent d'un délai de douze mois à compter de la publication de celle-ci pour mettre leur traitement en conformité.

La délibération n° 2006-067 du 16 mars 2006 portant adoption d'une norme simplifiée concernant les traitements automatisés de données à caractère personnel mis en œuvre par les organismes publics ou privés destinés à géolocaliser les véhicules utilisés par leurs employés et la délibération n° 2006-066 du 16 mars 2006 portant adoption d'une recommandation relative à la mise en œuvre de dispositifs destinés à géolocaliser les véhicules automobiles utilisés par les employés d'un organisme privé ou public sont abrogées.

Art. 9. – La présente délibération sera publiée au *Journal officiel* de la République française.

La présidente,
I. FALQUE-PIERROTIN