Recommandation n° 03/2013 du 24 avril 2013

Objet: Recommandation d'initiative concernant l'utilisation par les services de police de dispositifs de traçage à l'égard de leurs membres (CO-AR-2011-014)

La Commission de la protection de la vie privée ;

Vu la loi du 8 décembre 1992 *relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel* (ci-après LVP), en particulier l'article 30 ;

Vu le rapport de Monsieur Stefan Verschuere, Vice-président;

Émet, le 24 avril 2013, la recommandation suivante:

I. CONTEXTE

A. Utilisation des dispositifs de traçage dans la police

1. Depuis plusieurs années, les services de police installent sur leurs voitures ou confient à leurs membres des dispositifs de traçage permettant de les localiser ou de collecter, conserver, et analyser des données relatives à l'utilisation des véhicules ou des éléments qu'ils transportent (comme une arme ou un défibrillateur par exemple[1]). Les systèmes de traçage sont le plus souvent élaborés et proposés par des sociétés privées, mais peuvent également être développés en interne ou entre les services de police et d'autres services publics (comme la protection civile).

2. Certains dispositifs permettent uniquement de localiser les véhicules, alors que d'autres permettent de suivre l'utilisation d'un véhicule de manière beaucoup plus précise. Dans ce dernier cas, ces dispositifs peuvent être comparés des « boîtes noires » qui enregistrent une série de données relatives au véhicule.

3. Parmi les systèmes existants, on retrouve notamment les systèmes « AVL » (Automated Vehicule Location) qui permettent de localiser un véhicule (par GPS ou signal radio, comme c'est le cas avec le réseau ASTRID par exemple). Etant donné leur configuration, ces dispositifs sont toujours reliés à un membre du personnel, dès lors qu'ils sont activés par le conducteur par le biais d'un moyen d'authentification et/ou d'identification.

4. Il existe également d'autres dispositifs qui collectent plus de données, et permettent de retracer l'historique d'utilisation d'un véhicule. Les données collectées sont notamment celles qui suivent :

   - Les accélérations des véhicules
   - Les freinages brutaux
   - Les distances de freinage
   - Le déclenchement des feux
   - L'utilisation des sirènes
   - L'utilisation des feux de croisement
   - L'utilisation du gun lock
   - La détection d'impacts

[1] Le cas de la coopération entre les services de police et les pompiers pour localiser les défibrillateurs démontre que le traçage peut également concerner des activités qui ne sont pas les responsabilités premières de services de police.

- Les distances parcourues
- Les dates et heures de roulage
- La géolocalisation des véhicules
- L'historique des entretiens du véhicule

5. Des dispositifs de traçage portables permettent également de localiser un membre du personnel en particulier. Ces dispositifs sont utilisés pour localiser la section à laquelle appartient le membre des services de police, et sont utilisés principalement en cas d'opérations conjointes impliquant des membres de personnel issus de différents corps de police (différentes zones de police locale, ou police locale et fédérale).

6. Enfin, la Commission a pris connaissance d'un projet de collaboration entre la police et les pompiers. Ce projet permet de repérer les défibrillateurs qui seraient installés dans certains véhicules de police afin de déterminer, dans les situations d'urgence, où est l'appareil le plus proche du lieu où il doit être utilisé. Il est ainsi possible de faire appel aux services d'urgence les moins éloignés du lieu d'intervention. Le traçage de ce type n'est donc pas lié à une voiture mais plutôt au défibrillateur lui-même.

7. La Commission avait déjà été interrogée à ce sujet par la Police Fédérale en octobre 2011. Avant d'adopter la présente recommandation, la Commission a consulté la Commission Permanente de la Police Locale, la Police Fédérale, ainsi que le Comité P. Une réunion a également eu lieu le 12 novembre 2011 dans les locaux de la zone de Police de Bruxelles Nord en présence de la Police Fédérale pour discuter de l'expérience acquise suite à l'utilisation de systèmes de traçages déjà installés sur certains véhicules et des systèmes qui pourraient potentiellement être utilisés.

B. L'utilisation des données générées par les dispositifs de traçage

8. Les dispositifs de traçage peuvent être utilisés dans plusieurs contextes. Ainsi, dans leur **aspect opérationnel**, ceux-ci permettent de localiser les véhicules ou les équipes en temps réel. Il est ainsi possible de gérer les interventions au mieux en fonction des effectifs proches de l'événement, mais aussi de porter efficacement secours à une équipe en difficulté, ou encore de guider les véhicules, dans des événements prioritaires ou dans des opérations de police spécifiques telles que manifestations, épreuves sportives, etc. La localisation des défibrillateurs permet indiscutablement de gagner du temps pour secourir une personne.

9. Dans leur **aspect logistique**, les dispositifs de traçage (et notamment les systèmes de « gestion de flotte ») permettent d'entretenir et d'intervenir plus efficacement pour la réparation de certaines pièces ou organes mécaniques, mais aussi de gérer le parc automobile en prenant connaissance, par exemple, des distances parcourues par les véhicules ou des temps de conduite ou d'arrêt.

10. Certains systèmes de « gestion de flotte » peuvent également permettre **l'aide au conducteur**, par exemple au moyen d'un avertissement sonore pour éviter d'endommager les parties techniques, comme la poursuite de fonctionnement du moteur après une certaine durée, ou encore la faiblesse de la batterie.

11. Un dispositif peut également permettre d'assurer la **sécurité** du véhicule, lequel ne peut pas être démarré sans le badge d'activation, ce qui permet d'éviter le vol du véhicule. Le badge peut également être lié à un mécanisme de sécurité pour empêcher de s'emparer de l'arme de service attachée au véhicule.

12. Enfin, les dispositifs de traçage rendent possible le **contrôle** des utilisateurs (les membres des services de police) peut également être effectué, à charge ou à décharge de ces derniers. L'identification du conducteur permet par exemple, en cas de report d'incident, de déterminer qui était effectivement au volant lors de l'incident reporté. Ainsi, certains comportements non tolérés peuvent être identifiés et reliés à leur auteur, comme les freinages violents (révélant un style de conduite), les excès de vitesse (légitimes ou non), l'usage des feux bleus et de l'avertisseur sonore, ou la vitesse immédiate précédant un accident.

13. L'expérience des services de police ayant implémenté un tel système a conduit à constater une réduction sensible du nombre d'incidents et des cas usures prématurées (freins, pneus,..).[2] Il apparaît également que ces systèmes ont permis de recadrer certains comportements de conduite, ou encore de servir de preuves en cas d'incident survenu avec des tiers (usage ou non des gyrophares, vitesse de conduite,…).

14. Le transfert des données collectées et l'accès à ces dernières peut techniquement se faire de plusieurs manières. D'après les informations obtenues auprès des différentes zones de police, les modes de communication suivants sont les plus courants :

[2] Voy. par exemple Réponde du Ministre à la Question orale n° P1536 de Michel Doomst, *Chambre*, 52 PLEN 135.

- le premier consiste à transmettre toutes les informations de la « boîte noire » du véhicule par un support physique (clé USB ou badge) vers l'ordinateur de l'autorité policière en charge du traitement des informations. Dans ce premier cas de figure, les données ne sont pas traitées en externes ou accessibles à des fournisseurs extérieurs à la police ;
- le second consiste à transmettre les données collectées à une société fournissant la solution gestion de flotte[3] (le plus souvent par des solutions sans fil, comme par exemple via le réseau GSM par paquets GPRS) et de permettre un accès distant de ces données par l'autorité policière en charge via une application spécifique. Dans cette hypothèse, l'entreprise qui fournit le système (ou son sous-traitant) conserve les données pendant une certaine durée qu'elle détermine[4] ;
- enfin, les données peuvent également être transmises directement par transmission hertzienne et sans support physique au serveur de police sur un serveur interne, sans passer par un intermédiaire.

15. Des solutions informatiques et logiciels permettent de traiter les données, d'y accéder, et de réaliser des analyses de celles-ci, par exemple en créant des rapports globalisés ou détaillés (par chauffeur ou par véhicule). L'accès à ces données peut également se faire à distance, selon la configuration du système de traçage choisi et des configurations techniques.

II. OBJET DE LA PRESENTE RECOMMANDATION

16. La Commission constate que les données traitées visent à la fois l'utilisation des véhicules mais aussi le comportement des utilisateurs, à savoir les membres du corps de police. Dans certains systèmes existants, ces derniers doivent d'ailleurs s'identifier au moyen d'un badge lequel permet de démarrer le véhicule ou d'accéder à certains locaux des postes de police. Il s'ensuit donc que l'utilisation de badges liés aux systèmes de traçage peut s'inscrire dans un système plus large de contrôle. La présente recommandation ne se penchera pas sur ces systèmes particuliers.

[3] Ou du sous-traitant qu'elle choisit pour conserver les données.

[4] La Commission a reçu d'un fournisseur, à titre indicatif, l'information selon laquelle un prestataire de services de fleet management conservait les données pendant une année.

17. La Commission comprend que la police fédérale utilise déjà des dispositifs de traçage à l'occasion de certaines missions (comme les escortes de fonds) et que certaines zones de la police locale, quant à elles, utilisent également de tels systèmes.[5]

18. La Commission n'a pas de vue complète sur les différentes fonctions et utilisations des systèmes de traçage là où ils ont été mis en place jusqu'à présent. En effet, les différentes zones de police qui ont décidé d'implémenter de tels systèmes n'ont pas forcément choisi le même système, ni le même fournisseur. Il s'ensuit que ces services ne fonctionnent pas tous de la même façon, ne collectent pas tous les mêmes données, et ne présentent pas les mêmes caractéristiques.

19. Consciente du fait que ces dispositifs de traçage entraînent le traitement de nombreuses données, dont des données à caractère personnel, la Commission a estimé utile de préciser à quelles conditions l'usage de ces dispositifs de traçage au sein des services de police doit être encadré au regard de la LVP et d'émettre des recommandations pratiques à cet égard.

III. LOIS APPLICABLES

A. Droit fondamental repris à l'article 22 de la Constitution

20. L'article 22 de la Constitution prévoit que « Chacun a droit au respect de sa vie privée et familiale, sauf dans les cas et conditions fixés par la loi. La loi, le décret ou la règle visée à l'article 134 garantissent la protection de ce droit». Cet article doit être interprété à l'a lumière de l'article 8 de la C.E.D.H., lequel s'applique également sur le lieu de travail.[6]

B. Le secret des communications électroniques

21. Les **articles 314 bis et 259 bis du Code pénal** punissent respectivement quiconque (article 314 bis, §1) ou tout officier ou fonctionnaire public, dépositaire ou agent de la force publique qui, à l'occasion de l'exercice de ses fonctions, hors les cas prévus par la loi ou sans respecter les formalités qu'elle prescrit (article 259 bis, §1) qui :

---

[5] Réponse à la Question écrite de Dirk Claes n°4-6579 du 27 janvier 2010 à la Ministre de l'Intérieur, *Questions parlementaires*, Sénat, sess. 2009-2010 ; Question orale n° P1536 de Michel Doomst, *Chambre*, 52 PLEN 135.

[6] C.E.D.H., *Niemitz c. Allemagne*, 16 décembre 1992, Série A., n°251 ; C.E.D.H.*, Halford c. Royaume-Uni,* 25 juin 1997, *Rec.* III*,* p. 39.

- « soit, intentionnellement, à l'aide d'un appareil quelconque, écoute ou fait écouter, prend connaissance ou fait prendre connaissance, enregistre ou fait enregistrer, pendant leur transmission, des communications ou des télécommunications privées, auxquelles il ne prend pas part, sans le consentement de tous les participants à ces communications ou télécommunications;

- soit, avec l'intention de commettre une des infractions mentionnées ci-dessus, installe ou fait installer un appareil quelconque ».

22. L'**article 124 de la loi du 13 juin 2005** relative aux communications électroniques (ci-dessous « la LCE ») prévoit que *"s'il n'y est pas autorisé par toutes les personnes directement ou indirectement concernées, nul ne peut:*

1° prendre intentionnellement connaissance de l'existence d'une information de toute nature transmise par voie de communication électronique et qui ne lui est pas destinée personnellement ;

2° identifier intentionnellement les personnes concernées par la transmission de l'information et son contenu ;

3° sans préjudice de l'application des articles 122 et 133, prendre connaissance intentionnellement de données en matière de communications électroniques et relatives à une autre personne ;

4° modifier, supprimer, révéler, stocker ou faire un usage quelconque de l'information, de l'identification ou des données obtenues intentionnellement ou non."

23. Si les communications de données de localisation peuvent tomber, selon la Commission, dans le champ d'application de ces dispositions, il y a cependant lieu de considérer que l'article 124 de la LCE ne peut donc être opposé à l'autorité policière concernée, dès lors que les communications en question lui sont personnellement adressées.

24. En effet, la Commission a ainsi déjà considéré que l'article 124 de la LCE permet pour les destinataires du message de faire un usage légitime de l'information de la communication qui leur est personnellement destinée, sous réserve de respecter la LVP. [7]

C. Protection des données de localisation

[7] Voy. Recommandation n°07/2011 du 21 décembre 2011 concernant l'enregistrement des appels téléphoniques vers les commissariats et les hôpitaux ainsi qu'à partir de ceux-ci.

25. L'article 123 de la LCE ne permet l'utilisation des données de localisation par les opérateurs de réseaux mobiles que lorsqu'elles ont été rendues anonymes ou que le traitement s'inscrit dans le cadre de la fourniture d'un service à données de trafic ou de localisation.

26. Les données de localisation exploitées dans les systèmes de traçage ne sont pas concernées par ces dispositions, puisque ces données ne sont pas générées par un opérateur de réseau mobile, mais sont des données GPS provenant directement du terminal de géolocalisation.

27. La Commission avait déjà souligné cette distinction en concluant que *« les abonnés et utilisateurs utilisant ce type de services seraient donc protégés uniquement par la loi générale relative à la vie privée et non pas par les règles spécifiques additionnelles relatives aux communications électroniques. La protection offerte serait dès lors moindre pour les utilisateurs de ce type de service et il y aura une différence de protection selon que le service de localisation utiliser des données de localisation provenant d'un réseau de communication (sur base des antennes GSM, par exemple) ou d'une source externe au réseau (sur base des informations GPS, par exemple) ».*[8]

28. Il en résulte que l'article 123 ne s'applique pas aux dispositifs de traçage, dès lors que les informations de géolocalisation ne sont pas traitées par un opérateur de services de communications mais par un tiers, fournisseur de services basés sur les données de localisation fournies par la boîte noire du véhicule.[9] Le Groupe de l'article 29 est également d'avis que la Directive 2002/58/CE (aussi appelée « Directive e-privacy », dont l'article 9 est transposé en droit belge par l'article 123 de la LCE) ne s'applique pas à un tel traitement de données localisation, même si ce traitement a lieu via un réseau public de communications électroniques.[10]

D. Traitement des données à caractère personnel et application de la LVP

29. Les données de localisation des véhicules ou du matériel ou des appareils qui y sont reliés avec le conducteur et les passagers d'un véhicule constituent des données à caractère personnel au sens de la LVP dès lors que les informations sont susceptibles de concerner une personne identifiée ou identifiable au sens de l'article 1, §1 de la LVP. De même, les données de localisation d'une section, lorsqu'un appareil de géolocalisation est portée par un

[8] Avis n°18/2007 du 27 avril 2007 concernant la proposition de loi modifiant la loi relative aux communications électroniques en vue d'assurer une meilleures protection de la vie privée pour les « services à données de localisation » ou de services de « géolocalisation » par téléphone portable.

[9] Soit via une transmission sans fil au serveur du fournisseur de système de fleetlogging, soit par un transfert physique vers le système informatique du poste de police centralisant les données.

[10] Opinion 13/2011 adopted on 16 May 2011 on Géolocation services on smart mobile devices, WP 185, § 4.2.1.

de ses membres, génère des données à caractère personnel dès qu'il devient possible d'identifier les déplacements d'un membre des services de police.

30. Les dispositions de la LVP s'appliqueront au traitement des données générées par les dispositifs de traçage, dès lors que ces dernières sont des données à caractère personnel au sens de l'article 1 §1 de la LVP et que le traitement est entièrement automatisé.[11]

31. La présente recommandation examinera la conformité avec la LVP des systèmes de traçage utilisés dans les services de police, cette loi étant le texte de référence applicable en la matière pour ce qui concerne le traitement des données à caractère personnel.

IV. PRINCIPES A RESPECTER AU REGARD DE LA LVP

1. Finalités

32. En vertu de l'article 4, §1, 2° de la LVP, tout traitement de données à caractères personnel, tel qu'un système de traçage, doit répondre à des finalités déterminées, explicites et légitimes qui en justifient son installation et son utilisation.

33. La Commission relève plusieurs finalités, poursuivies actuellement au sein des services de police, qui peuvent être retenues dans le cadre de l'utilisation des données de traçage et qui peuvent être considérées comme légitimes :

- **Sécurité des véhicules et des membres des services de police :** les systèmes de traçage permettent notamment par exemple de s'assurer que les membres des services de police sont localisables en cas de problèmes ou de difficulté (en cas d'absence ou impossibilité de communiquer à la centrale) ; certains dispositifs permettent également d'empêcher que les armes attachées aux véhicules ou que le véhicule soient utilisées par des personnes non autorisées ;

- **Gestion du parc automobile :** certains dispositifs de traçage permettent de suivre l'état du parc automobile, et d'identifier les besoins d'entretien, de remplacement ou de maintenance. Au niveau individuel, le conducteur peut également recevoir des informations utiles, comme un avertissement sonore en cas de batterie faibles, de pièces défectueuses, ou d'une utilisation anormale du moteur ;

[11] Article 3 de la LVP.

- **Gestion opérationnelle dans le cadre des missions de police:** la localisation en temps réel permet d'assurer une meilleure efficacité des interventions des effectifs en présence mais aussi de localiser une équipe en difficulté. Cette finalité se recoupe évidemment à plusieurs égards avec celle relative à la sécurité des membres des services de police et des véhicules ;

- Enfin, le **contrôle** des utilisateurs (les membres du personnel de police) est également rendu possible par certains dispositifs de traçage. A l'aide de ces derniers, les membres des services de police peuvent être contrôlés à la fois quant à l'utilisation qu'ils ont fait du véhicule (freinages brusques, heures et durées d'utilisation, vitesse, utilisation intempestive des gyrophares,…) mais également eu égard à leurs déplacements, grâce à la géolocalisation.

- En outre, les données disponibles pourraient être utilisées – à charge ou à décharge - en cas de **plainte concernant le comportement d'un membre des services de police** dans ses relations avec les individus (par exemple en cas d'accident, ou d'arrivée tardive sur les lieux,..). L'utilisation de ces données dans le cadre de procédures disciplinaires ou encore judiciaires constitue donc une autre finalité envisageable.

34. La Commission constate que, vu la spécificité des missions de police, ces finalités doivent être considérées comme légitimes, au regard des impératifs de sécurité, d'efficacité, et d'organisation auxquels les services de police doivent répondre. Cependant, ces finalités, prises ensemble ou séparément, ne sauraient automatiquement être reconnues comme légitimes dans d'autres secteurs, publics ou privés, sans une analyse concrète des hypothèses impliquant un traitement de données des employés.

35. La Commission rappelle également que les données collectées ne peuvent être utilisées pour d'autres finalités avec celles qui auront été déterminées de manière précise préalablement au traitement envisagé, compte tenu de tous les facteurs pertinents, notamment des prévisions raisonnables de l'intéressé et des dispositions légales et règlementaires applicables.[12] Il appartiendra évidemment aux responsables du traitement d'apprécier si l'utilisation des données (notamment à des fins de poursuite pénales ou disciplinaires) est compatible avec la collecte initiale de ces données, en fonction facteurs pertinents, et notamment de l'information communiquée aux personnes concernées.

[12] Article 4, 2° de la LVP.

36. En outre, la Commission rappelle que l'annonce des finalités pour lesquelles les données sont utilisées permettra de déterminer le délai de conservation de ces données, conformément aux principes exposés dans la présente recommandation aux points 64 et suivants.

2. Admissibilité du traitement

37. Un traitement de données à caractère personnel ne peut être effectué que dans un nombre limité de cas, énumérés par l'article 5 de la LVP.

38. La Commission estime que se baser sur le consentement du travailleur comme fondement de légitimité d'un traitement sur la base de l'article 5, *a)* de la LVP dans le cadre de relations de travail n'est pas sans poser problème. En effet, dans ce contexte particulier, il ne se pose pas dans un rapport de forces équilibré alors que le consentement exigé doit être libre et éclairé. [13]

39. La Commission estime toutefois que la base de légitimité, dans ce cas précis, trouve son fondement sur les autres hypothèses d'admissibilité du traitement reprises aux literas *c), e)* ou *f)* de l'article 5.[14]

40. **Concernant les finalités relatives à la sécurité des véhicule et des membres des services de police, la gestion du parc automobile, et la gestion opérationnelle,** la Commission estime que le traitement des données est admissible en vertu des literas *c)* et *e)* de la l'article 5 de la LVP. En effet, le traitement des données générées par les dispositifs de traçage permet aux services de police de remplir leurs missions légales et d'assurer leur mission d'intérêt public qui leur sont confiées par la loi.[15] Les données traitées par les systèmes de traçage permettent aux services de police de réaliser leurs missions avec l'efficacité et dans les conditions optimales que les individus sont en droit d'attendre de la part de tels services, de par les missions d'intérêt public qu'ils exercent.

---

[13] Recommandation d'initiative n°08/2012 du 2 mai 2012 relative au contrôle de l'employeur quant à l'utilisation des outils de communication électronique sur le lieu de travail, pt. 53.

[14] Voy. Opinion 13/2011 du Groupe de l'article 29 déjà citée, ainsi que la Recommandation d'initiative de la Commission n°07/2011 du 21 décembre 2011 concernant l'enregistrement des appels téléphoniques vers les commissariats de police et les hôpitaux ainsi qu'à partir de ceux-ci, points 22 et suivants.

[15] Les autorités de polices doivent en effet assurer le respect des diverses missions qui leur sont assignées par la loi. Voy. ainsi la loi du 7 décembre 1998 organisant un service police intégré, structuré à deux niveaux, et plus spécifiquement les articles 44, 97, 98, 99, 120, 124, l'arrêté royal du 10 mai 2006 fixant le Code de déontologie des services de police, la loi du 13 mai 1999 portant le statut disciplinaire des membres du personnel des services de police, l'arrêté royal du 26 novembre 2001 portant exécution du statut disciplinaire des membres du personnel des services de police.

41. **Concernant les finalités de contrôle et gestion des plaintes relatives au comportement d'un membre des services de police,** la Commission estime que le traitement des données est admissible en vertu du litera *f)* de l'article 5 de la LVP. La finalité de contrôle des membres du personnel permet de s'assurer que des abus n'ont pas lieu dans l'utilisation des véhicules (dépassement de vitesse non justifiés, utilisation abusive de gyrophares, utilisation intempestive des sirènes,…), mais encore de se ménager un moyen de preuve en cas de contestation relative au comportement d'un membre du personnel.

42. La Commission constate en outre que l'intérêt légitime poursuivi par les services de police dans le cadre des traitements examinés se confond en partie avec celui de la société, laquelle requiert une certaine efficience logistique, une gestion efficace des moyens publics, et un exercice adéquat de la mission d'intérêt public dont sont investis les services de police. Pour ces raisons, la balance des intérêts réalisée en vertu de l'article 5 *f)* de la LVP permet de conclure à l'admissibilité du traitement pour les finalités de contrôle et de gestion des plaintes.

43. Eu égard à ce qui précède, la Commission considère que les traitements décrits ci-dessus sont admissibles en vertu de l'article 5 *f)* en ce qui concerne la finalité de contrôle et de gestion des plaintes, et de l'article 5 *c)* et *e)* pour ce qui concerne les autres finalités.

3. Proportionnalité

44. En vertu de l'article 4, 3° de la LVP les données traitées doivent être adéquates, pertinentes et non excessives. Cela signifie que les données de ce traitement doivent se limiter à ce qui est strictement nécessaire pour réaliser la ou les finalité(s) ainsi déterminées.

45. En outre, le traitement des données collectées (géolocalisation, vitesse, freinages, fonctionnement du gyrophare, détection d'impacts, etc.) ne peut porter atteinte à la vie privée des membres des services de police de manière disproportionnée eu égard aux objectifs légitimes poursuivis par le responsable du traitement et rappelés ci-dessus.

46. En ce qui concerne la **finalité de contrôle** des activités des membres des services de police, la Commission précise que ce contrôle ne peut s'effectuer que dans des circonstances bien encadrées. Les contrôles systématiques et/ou individualisés ne peuvent être la norme de principe et doivent constituer l'exception.

47. En effet, un **contrôle permanent** des données d'un membre du personnel de police ne pourra avoir lieu que dans des cas justifiés par le responsable du traitement. L'analyse des

données concernant le comportement ou les activités du membre ne sera légitime que si des indices sérieux laissent présager un comportement répréhensible, inadéquat ou interdit, ou si des circonstances particulières justifient les recherches dans les données collectées. On pensera par exemple à un accident survenu avec le véhicule en cas de doute sur la véracité des récits des personnes impliquées, ou encore à l'hypothèse d'usure anormale d'un véhicule, ou de plaintes ou indices convergentes concernant des interventions policières abusives ou l'utilisation abusive du matériel policier (gyrophares, sirènes, vitesse de conduite,..).

48. **En ce qui concerne les finalités autres que le contrôle**, sera également considéré comme proportionné le suivi en temps réel des voitures et des leurs occupants sur base des données de géolocalisation pour assurer l'efficacité des interventions. Il en sera de même de l'analyse de données globalisées et non individualisées qui permettrait au responsable du traitement de se rendre compte de l'état des véhicules, de l'usure d'un véhicule, ou du nombre de kilomètres parcouru en moyenne par véhicule.

49. *A contrario*, seront considérés comme disproportionnées, la conservation et l'analyse automatiques des données à des fins de contrôles systématiques et non ciblés des membres du personnel des services de police.

50. De même, la désactivation des fonctions de localisation devrait être prévue dans le cas de l'utilisation par un membre de la police d'une voiture de service en dehors des heures de service, par exemple dans l'hypothèse où il aurait ramené le véhicule chez lui en prévision d'une réunion de travail ayant lieu le lendemain. Le traçage permanent de ce véhicule en dehors des heures de service pourra être considéré comme disproportionné alors que d'autres moyens plus appropriés pourront dans ce cas précis être mis en œuvre pour repérer le véhicule, comme le signalement à la hiérarchie ou au dispatching de l'utilisation du véhicule pour les besoin du service en dehors des heures de fonction.

51. La Commission n'exclut pas que d'autres hypothèses puissent exister dans lesquelles une analyse individualisée des données justifie, mais elles devront être appréciés au cas par cas.[16]

52. Dans le cadre où les données collectées seraient utilisées pour contrôler l'activité du membre du service de police au niveau disciplinaire, il convient de rappeler que le supérieur

[16] On pensera notamment au contrôle des interventions des patrouilles, pour s'assurer de leur présence sur les lieux, ou pour assurer le respect de consignes données aux membres des services de police et qui n'ont pas été respectées, après notification qu'un contrôle de leurs activités allait avoir lieu à cet égard.

hiérarchique du membre des services de police devra le convoquer si un incident a été reporté le concernant, afin de lui permettre de fournir ses explications à ce sujet. Une interprétation des données brutes et l'application immédiate d'une sanction, sans laisser à la personne concernée la possibilité de donner son interprétation des données de traçage la concernant, constituent des actes susceptibles de violer le principe du contradictoire, mais également l'article 12*bis* de la LVP.

4. Transparence

53. Conformément à l'article 9, §1 de la LVP, la Commission rappelle que les membres des services de police doivent être informés, préalablement à tout traitement, des éléments essentiels concernant le traitement effectué sur base des données à caractère personnel les concernant.[17]

54. Ainsi, la Commission recommande que les données suivantes au moins soient communiquées aux membres des services police concernés:

- Identité du responsable de traitement (par exemple, le chef de la zone de police concernée) ;
- Les finalités du traitement ;
- Le type de données traitées ;
- La durée de conservation des données ;
- Les destinataires de ces données ;
- L'existence d'un droit d'accès, de rectification et de suppression et les modalités pour leur mise en œuvre ;
- L'identité ou la fonction des personnes accédant ou pouvant accéder à ces données ;
- Les modalités de consultation (par qui, à quelle fréquence, dans quels cas) ;
- Les modalités du traitement envisagé (par exemple : information sur la périodicité et l'existence d'un enregistrement ponctuel ou systématique, information sur l'éventuelle désactivation du système quand le membre des services de police rentre chez lui et la procédure à suivre).

55. Ces informations peuvent être données sur tout support utile (notes de services, circulaires internes, email, voie d'affichage, intranet, etc.) qui sera jugé approprié par le chef du service

[17] Recommandation d'initiative de la Commission n°07/2011 du 21 décembre 2011 concernant l'enregistrement des appels téléphoniques vers les commissariats de police et les hôpitaux ainsi qu'à partir de ceux-ci, points 30 et suivants.

de police concerné pour que la prise de connaissance par toutes les personnes concernées par le traitement soit garantie.

56. La Commission recommande, pour ce type de traitement de données, une concertation préalable avec les organisations syndicales du secteur professionnel concerné afin de les informer au mieux du traitement et des finalités poursuivies.

57. D'ailleurs, la règlementation syndicale en matière de police associe les organisations syndicales à l'adoption de mesures relatives à l'organisation du travail, dans une procédure de concertation préalable.[18]

5. Droit d'accès, de rectification et de suppression

58. En vertu de l'article 10 de la LVP, les personnes concernées disposent d'un droit d'accès relatif aux données qui les concernent, obligeant notamment le responsable du traitement à communiquer sous forme intelligible les données faisant l'objet d'un traitement.

59. L'article 12 de la LVP reconnaît également un droit d'opposition dans certains cas précis[19], un droit de rectification des données inexactes, incomplètes ou non pertinentes et un droit de suppression si les données sont conservées pour une durée supérieure à celle nécessaire à la finalité pour laquelle elles sont traitées.

60. La Commission confirme que ce droit d'accès doit être effectivement rendu possible à l'égard des membres des services de police dont les données sont traitées. Ils devront être informés de la personne auprès de laquelle ils pourront adresser une demande d'accès pour prendre connaissance des données traitées les concernant.

61. En outre, s'il s'avère que les données traitées sont inexactes, les membres des services de polices pourront faire valoir leur droit de rectification, après avoir démontré que la donnée doit être corrigée.

---

[18] Loi du 24 mars 1999 organisant les relations entre les autorités publiques et les organisations syndicales du personnel des services de police (articles 6 à 8) ; Arrêté royal du 8 février 2001 déterminant les règlementations de base au sens de l'article 3, alinéa 1er, 1° de la loi du 24 mars 1999 précitée.

[19] La personne concernée doit démontrer qu'elle des raisons sérieuses et légitimes tenant à une situation particulière pour s'opposer au traitement de ses données.

62. Les membres des services de police pourront également demander la suppression de données les concernant et dont la conservation n'est plus justifiée par les besoins pour lesquels cette donnée avait été initialement traitée (voir point 6 ci-dessous, concernant la durée de conservation).

6. Durée de conservation des données

63. Les données ne peuvent être traitées pour une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont obtenues ou pour lesquelles elles sont traitées ultérieurement.[20]

64. Il en ressort que la durée de conservation des données doit être limitée dans le temps, être proportionnelle à l'utilisation qui est faite des données et déterminée par le responsable du traitement pour chacune des finalités.

65. En application de ces principes, la donnée attestant de la présence de tel ou tel membre des services de police sur les lieux devrait être soumise à un traitement d'une durée moindre que celle permettant de réaliser des statistiques sur l'utilisation d'un véhicule pendant sa durée de vie.

66. De la même manière, des données qui pourraient être utilisée pour sanctionner pénalement ou disciplinairement un membre des services de police ne pourront être gardée plus longtemps que le délai de prescription de l'action pénale ou disciplinaire, à moins que d'autres finalités puissent justifier une conservation plus longue.

67. Vu les nombreuses finalités poursuivies par les systèmes de traçage et la multitude des délais de conservation qui pourraient en découler, la Commission estime qu'une seule période de conservation de six mois peut être considéré comme proportionné. Il ressort d'ailleurs des informations de la Commission que cette période est celle qui est retenue par les services de police et correspond par ailleurs au délai de prescription en matière disciplinaire. La Commission n'exclut pas toutefois qu'un délai de conservation plus long puisse être justifié dans des circonstances particulières et notamment dans le cas d'une information ou d'une instruction judiciaire. Le service de police devra néanmoins avancer les éléments qui justifient une telle conservation supérieure à 6 mois.

---

[20] Article 5, 5° de la LVP.

68. Cependant, les données qui auraient été anonymisées, c'est-à-dire qui ne peuvent plus être liées à un individu, pourront quant à elle être conservées pour une période plus longue, dès lors qu'elles ne sont plus des données à caractère personnel et ne sont plus soumises à la LVP.

7. Sécurité des données

69. La Commission souligne l'importance du respect du principe de sécurisation des traitements de données à caractère personnel, prévu à l'article 16 de la LVP, qui impose au responsable du traitement de prendre toutes les mesures techniques et organisationnelles adéquates requises pour protéger les données contre la destruction accidentelle ou non autorisée, contre la perte accidentelle ainsi que contre la modification, l'accès et tout autre traitement non autorisé de données à caractère personnel. Le caractère adéquat de ces mesures de sécurité dépend, d'une part, de l'état de la technique et des frais engendrés et d'autre part, de la nature des données à protéger et des risques potentiels. Le responsable du traitement doit tenir compte des «mesures de référence en matière de sécurité applicables à tout traitement de données à caractère personnel»[21] et des « lignes directrices pour la sécurisation des données à caractère personnel » qui sont publiées sur le site web de la Commission. Cette dernière renvoie également à cet égard à sa Recommandation n°01/2013 relative aux mesures de sécurité à respecter afin de prévenir les fuites de données.[22]

70. Le responsable du traitement doit désigner de manière limitative les personnes dont l'accès aux données en question est rendu strictement nécessaire pour réaliser le traitement. Seules les personnes ayant un intérêt fonctionnel pourront donc accéder aux données et les traiter. Cela signifie également que des moyens logistiques, techniques mais aussi organisationnels devront être mis en œuvre pour empêcher que les données en question soient accessibles à d'autres personnes que celles ainsi désignées. [23]

71. Le responsable du traitement doit également faire toute diligence pour tenir les données à jour, pour rectifier ou supprimer les données inexactes, incomplètes, ou non pertinentes, ainsi que celles obtenues ou traitées en méconnaissance des articles 4 à 8 de la LVP. Il doit également veiller à ce que, pour les personnes agissant sous son autorité, l'accès aux

---

21 http://www.privacycommission.be/sites/privacycommission/files/documents/mesures_de_reference_en_matiere_de_securite_applicables_a_tout_traitement_de_donnees_a_caractere_personnel.pdf

22 Recommandation d'initiative du 21 janvier 2013.

23 On pense aux chefs de corps, directeurs, autorités disciplinaires, aux autorités de contrôle et de tutelle des services de police, ainsi qu'aux autorités judiciaires.

données et les possibilités de traitement soient limités à ce dont ces personnes ont besoin pour l'exercice de leurs fonctions ou à ce qui est nécessaire pour les nécessités du service.[24] Ceci suppose donc que les accès aux données en questions soient sécurisés et uniquement réservés aux personnes habilitées à les consulter.

72. Le responsable du traitement doit enfin s'assurer de la conformité des programmes servant au traitement automatisé des données à caractère personnel avec les termes de la déclaration faite à la Commission.[25]

73. Pour les zones de la police locale, la Commission recommande au responsable du traitement de désigner une personne de contact au sein de chaque zone, à laquelle la Commission pourra s'adresser concernant le traitement des données collectées par les dispositifs de traçage.[26]

74. Si responsable du traitement[27] choisit un sous-traitant, ce dernier devra apporter des garanties suffisantes au regard des mesures de sécurité technique et d'organisation relatives aux traitements.[28] Cette obligation est d'autant plus importante dès lors qu'on constate que ce sont souvent des sociétés privées qui traitent des données qui devraient faire l'objet d'une protection particulière puisqu'elles se rapportent à l'activité des services de police. Le choix du prestataire externe est donc primordial pour s'assurer que les données ne seront pas accessibles par un tiers, et seront prémunies contre tout accès non autorisé.

75. D'ailleurs, la Commission rappelle que la relation entre le responsable du traitement et une société fournissant des solutions de traçage doit faire l'objet d'un contrat écrit. En outre, le contrat devra déterminer la responsabilité du sous-traitant à l'égard du responsable du traitement, et mentionner que le sous-traitant ne peut agir que sur la seule instruction du responsable du traitement et est tenu par les mêmes obligations que celles auxquelles le responsable du traitement est tenu en application de l'article 16 § 3 de la LVP.[29]

---

[24] Article 16, §2 de la LVP.

[25] Article 16, §2 de la LVP.

[26] Conformément à l'article 44/2 de la loi du 5 août 1992 sur la fonction de police.

[27] En l'occurrence la Police Fédérale, ou, en ce qui concerne la police locale, la zone de police.

[28] Article 16, § 1 de la LVP.

[29] Lequel stipule que « toute personne agissant sous l'autorité du responsable du traitement ou celle du sous-traitant, ainsi que le sous-traitant lui-même, qui accède à des données à caractère personnel, ne peut les traiter que sur instruction du responsable du traitement, sauf en cas d'une obligation imposée par ou en vertu d'une loi, d'un décret ou d'une ordonnance ».

76. Ces consignes de sécurité obligent donc le service de police concerné à prendre toutes les mesures appropriées pour garantir la sécurité des données traitées pour son compte par le sous-traitant. En effet, la responsabilité du responsable du traitement reste engagée dans toutes les hypothèses.

8. Déclaration du traitement

77. Enfin, la Commission rappelle que tout traitement de données doit faire l'objet d'une déclaration conformément à l'article 17 de la LVP. Le traitement de données de traçage management doit donc faire l'objet de cette déclaration par toute autorité de police qui met en œuvre un tel traitement, dès lors que lesdits traitements ne sont pas exemptés de cette obligation. En effet, ils ne rentrent pas dans les hypothèses de la section II, Chapitre VII de l'arrêté royal du 13 février 2001 portant exécution de la LVP.

CONCLUSION

La Commission recommande que tous les principes exposés ci-dessus et que le prescrit de la LVP soient pleinement respectés lorsqu'un système de traçage est implémenté par un corps de police, eu égard en particulier aux principes de proportionnalité du traitement effectué, de transparence et d'information des membres du personnel des services de police, de durée de conservation des données collectées, mais également de sécurisation du traitement.

Elle recommande dès lors :

1. Que les données collectées par les systèmes de traçage se limitent aux données adéquates, pertinentes et non excessives à la poursuite de la ou des finalités annoncée(s) ;
2. Que chaque responsable du traitement identifie clairement les finalités pour lesquelles il met en place un dispositif de traçage ;
3. Que les données collectées par les systèmes de traçage ne soient pas utilisées à des fins de contrôles du personnel de manière permanente et que l'utilisation des données à des fins de surveillance et de contrôle soit adéquatement encadrée par un règlement de travail ou par un instrument équivalent ;
4. Que les membres du personnel de police soient clairement informés, par tout moyen adéquat, des données à caractère personnel collectées à leur sujet, ainsi que des finalités poursuivies par le traitement de ces données, les modes d'accès, de contrôle, la

durée de conservation ainsi que les autres informations identifiées au point 55 de la présente recommandation ;

5. Que le traitement des données collectées par le système de traçage fasse l'objet d'une déclaration auprès de la Commission, en mentionnant notamment la ou les finalités poursuivies ;
6. Que la durée de conservation des données à caractère personnel collectées au moyen des dispositifs de traçage soit de six mois sauf circonstances particulières justifiant une conservation plus longue ;
7. Que les mesures de sécurité adéquates soient adoptées par les services de police mettant en place de tels systèmes de traçage, et qu'un contrat écrit régisse les relations éventuelles avec un fournisseur externe, conformément aux points 70 et suivants de la présente recommandation et que ces mesures portent notamment sur les modalités d'accès aux données et sur la journalisation des accès.

L'Administrateur f.f., Le Président,

(sé) Patrick Van Wouwe (sé) Willem Debeuckelaere