Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Préposé fédéral à la protection des données et à la transparence (PFPDT)

Systèmes de localisation de personnes

On recourt de plus en plus aux systèmes de localisation de personnes, par exemple pour optimiser les flux de trafic ou de personnes, ou pour analyser le comportement des clients, notamment à des fins de marketing. Ces systèmes permettent même, dans certains cas, de recueillir des données sensibles ou d'établir des profils de la personnalité. Voilà pourquoi il convient de faire preuve de prudence lors de leur utilisation.

Vous trouverez ci-après des explications concernant les principaux aspects de la protection des données auxquels il faut veiller quand il s'agit de localiser des personnes.

Traitement de données personnelles par des systèmes de localisation de personnes

On peut en principe enregistrer les déplacements d'une personne ou d'un objet (p. ex. un véhicule) de deux façons: soit en détectant la personne ou l'objet et en suivant ses mouvements (surveillance spatiale), soit en détectant à un endroit précis (p. ex. à l'entrée d'un centre commercial ou à l'entrée d'une autoroute) certaines caractéristiques de la personne ou de l'objet en mouvement de façon à pouvoir les reconnaître aux points de contrôle suivants et retracer ainsi les déplacements effectués. Alors que la première façon nécessite d'énormes moyens, en particulier dans le cas de projets à grande échelle, si bien qu'elle est très rarement utilisée, la seconde façon est plus facile à mettre en œuvre, raison pour laquelle les systèmes recourant à cette méthode se multiplient sur le marché.

Face à cette situation, nous avons analysé quelques-uns de ces systèmes, ce qui nous a permis d'en identifier deux grands types :

1. Le premier type de systèmes répertorie directement des caractéristiques personnelles telles que les données biométriques du visage ou les plaques d'immatriculation des véhicules pour pouvoir reconnaître des personnes ou des véhicules quand ils passent à des points de contrôle. Il offre aussi souvent la possibilité de classer les personnes identifiées dans des catégories telles que l'âge, le sexe ou l'origine ethnique. Il ne fait dès lors aucun doute que l'utilisation de systèmes de ce type entraîne le traitement de données personnelles.

2. Le second type de systèmes répertorie les données des téléphones portables des personnes qui passent à proximité (numéro IMSI, numéro TMSI ou adresse MAC) et enregistre ainsi les déplacements des personnes qui portent ces appareils. Les opérateurs de ces systèmes affirment régulièrement qu'ils ne recueillaient pas de données personnelles, raison pour laquelle ils ne tombaient pas sous le coup de la loi fédérale sur la protection des données.
   Ces affirmations sont cependant imprécises: il est certes exact que les opérateurs de systèmes de ce type ne sont pas en mesure, pour l'instant, d'identifier directement une personne sur la base d'un numéro IMSI ou TMSI ou d'une adresse MAC. Mais, suivant les conditions, il serait possible de le faire dans le cas des profils de déplacement qui ont été établis. Ainsi, par exemple, les profils de déplacement du personnel d'un magasin sont en règle générale très différents de ceux de la clientèle. Dans le cas d'un magasin relativement petit, il est facile d'identifier un collaborateur précis grâce au profil de ses déplacements. Par ailleurs, la mise en relation des données recueillies, mais aussi des profils établis, avec d'autres données (p. ex. les images prises par les caméras de surveillance ou les données relatives au trafic des paiements) peut permettre l'identification d'une personne précise. Par conséquent, il faut considérer que, dans le cas de ces systèmes, on est en présence d'un traitement de données personnelles au sens de la loi fédérale sur la protection des données.

Comme il y a traitement de données personnelles dans le cas des deux types de systèmes, il doit toujours exister un **motif justificatif** pour qu'un système de localisation de personnes puisse être utilisé. Il peut s'agir, en l'occurrence, d'un intérêt public ou privé prépondérant ou du consentement des personnes concernées.

Consentement des personnes concernées

Dans les faits, il est souvent difficile de recueillir le consentement (juridiquement valable) des personnes concernées, car elles doivent être dûment informées de la collecte des données en question, mais aussi du traitement qui en sera fait, avant de pouvoir donner leur consentement (à ce propos, voir aussi la rubrique ci-dessous intitulée «Information des personnes concernées»). Dans les endroits très fréquentés où les personnes ne cessent de se déplacer, il est difficile d'informer dûment les personnes concernées de façon à ce qu'elles prennent véritablement la mesure desdites informations. Car le consentement n'a aucune validité juridique si les informations n'ont pas été données préalablement et si leur portée ne peut pas être identifiée ou évaluée.

Qui plus est, le consentement doit être libre: il ne peut être question de liberté que si les personnes concernées disposent d'une autre possibilité, qui soit équivalente, par exemple celle de se déplacer dans un centre commercial sous surveillance sans être répertoriées par les systèmes de localisation. Si leur seule possibilité est de ne pas pénétrer dans le centre commercial, on ne peut pas parler de liberté au sens juridique du terme. C'est la raison pour laquelle un consentement donné de cette façon est nul. En revanche, on pourrait envisager le recours à ce que l'on appelle une «liste blanche» (liste, pouvant être lue par le système, des personnes ou des téléphones portables qui ne doivent pas faire l'objet d'une localisation) pour empêcher des systèmes de localisation de répertorier des personnes n'ayant pas donné leur consentement.

Un consentement qui a été donné peut être révoqué à tout moment. C'est pourquoi il faut veiller à ce que les données relatives aux personnes qui révoquent leur consentement puissent être effacées ultérieurement.

Il faut par conséquent définir des processus d'effacement et désigner les personnes responsables de la procédure d'effacement.

Intérêt public ou privé prépondérant

Dans les cas où il n'est pas possible de recueillir un consentement juridiquement valable, il faut qu'il y ait un intérêt public ou privé prépondérant pour pouvoir exploiter un système de localisation de personnes. En règle générale, on est en présence d'un intérêt prépondérant lorsque les données personnelles sont traitées à des fins ne se rapportant pas à des personnes (art. 13, al. 2, let. e, LPD). Si un système de localisation de personnes est utilisé par exemple pour l'analyse des flux de personnes dans le but d'améliorer la sécurité dans les aéroports ou dans les gares, on peut présumer qu'il existe un intérêt public prépondérant pour autant qu'on ne procède pas, en l'occurrence, à l'analyse du comportement de personnes précises. Il en va de même pour l'analyse des flux de trafic sur les autoroutes dans le but de prévenir les embouteillages.

Il est possible d'invoquer un intérêt privé prépondérant par exemple s'il est prévu d'utiliser le système de localisation pour mesurer les fréquences de passage des clients ou pour analyser le comportement moyen des catégories de clients. Par contre, il n'y a pas, en règle générale, de motif justificatif dans le cas d'études portant sur le comportement de personnes précises - dont le nom n'est pas forcément connu - quand il s'agit par exemple d'envoyer des publicités personnalisées.

Dans chaque cas où la localisation ne porte pas sur des personnes, il faudrait respecter les règles suivantes:

- Les données se rapportant à des personnes doivent être effacées ou anonymisées le plus tôt possible. L'établissement d'un profil ne devrait pas se faire sur une longue période.
- L'étude doit être menée à l'aide de catégories qui ne permettent pas d'identifier des personnes en particulier. Une identification est toujours possible lorsqu'une catégorie ne comporte qu'une seule personne ou lorsqu'une seule personne correspond à une

combinaison précise de catégories. Il s'agit donc d'agréger les données de telle sorte qu'il soit impossible d'établir un lien avec une personne précise.
- Les données ne devraient pas être combinées avec d'autres données. Cette règle vaut aussi bien pour la combinaison avec d'autres données provenant du même environnement (p. ex. la combinaison du profil de déplacement avec les images prises par les caméras de surveillance ou avec les données qui concernent le trafic des paiements) que pour la combinaison avec des données provenant d'autres sources (p. ex. la combinaison des données du centre commercial A correspondant au jour X avec les données du centre commercial B correspondant au jour Y) étant donné que chaque combinaison fait augmenter les possibilités d'identification.

Information des personnes concernées

Indépendamment de la question de savoir si l'utilisation d'un système de localisation de personnes est légitimée par un intérêt prépondérant ou par le consentement des personnes concernées, il faut que ces dernières aient été au préalable dûment informées de la manière dont les données recueillies par le système de localisation seront traitées. À cet égard, il y a toute une série d'exigences à remplir:

- Les personnes concernées doivent être informées de l'existence du système de localisation avant de pénétrer dans le périmètre où ce système est en service. La meilleure solution consiste à placer des panneaux bien visibles indiquant au minimum que toutes les personnes entrant dans le périmètre en question seront répertoriées et que leurs déplacements seront enregistrés.
- Il faut élaborer une documentation-type qui renseigne sur les principaux aspects du traitement des données personnelles en rapport avec le système de localisation. La documentation doit pouvoir être consultée sur place et doit être remise aux personnes concernées qui le demandent, et même spontanément si le motif justificatif est un consentement.
- Il faut non seulement définir les procédures régissant l'octroi du droit d'accès et d'un éventuel droit à l'effacement, mais aussi désigner les

personnes responsables de la mise en œuvre de ces procédures. Il faut veiller à ce que les personnes concernées puissent faire un usage rapide, non bureaucratique et gratuit de leur droit d'accès et de leur droit à l'effacement.

Mesures supplémentaires à prendre en cas d'utilisation de données biométriques

Quelques systèmes de localisation utilisent des données biométriques pour identifier des personnes précises et enregistrer leurs déplacements (il s'agit en règle générale de systèmes de reconnaissance faciale). Le traitement de ces données recèle un risque élevé de violation de la personnalité étant donné qu'elles sont liées directement et durablement à une personne et qu'elles ne peuvent pas être modifiées ou remplacées en cas d'abus. C'est la raison pour laquelle il faut faire preuve d'une prudence toute particulière lors de l'utilisation de ces données (voir aussi notre guide relatif aux systèmes de reconnaissance biométrique et son complément).

Les règles suivantes s'appliquent dans les cas où des systèmes de localisation de personnes utilisent des données biométriques :

- Il est interdit d'utiliser des données biométriques brutes. Il suffit d'utiliser des modèles de référence (gabarits), lesquels contiennent beaucoup moins d'informations sur les personnes concernées, présentant ainsi un faible risque d'abus; dans ces conditions, il serait disproportionné d'utiliser des données brutes. Plusieurs systèmes examinés par nos soins ont par ailleurs montré qu'il n'est pas nécessaire que les gabarits utilisés se présentent sous une forme qui puisse être lue de façon générale. Voilà pourquoi ils doivent être transformés aussi rapidement que possible en une valeur de hachage de façon à ce qu'il soit encore plus difficile de tirer des conclusions sur les caractéristiques des personnes concernées.
- Les données doivent être effacées ou anonymisées le plus tôt possible. Comme il est interdit d'établir des profils de déplacement pendant une période prolongée , il serait disproportionné de stocker des données biométriques pendant une longue durée . Même si ces

données sont utilisées en relation avec une liste blanche, il faut fixer une durée de stockage maximale au terme de laquelle les données doivent être effacées de façon définitive.

- Si les données biométriques sont stockées de manière centralisée, il doit être impossible d'établir un rapport avec d'autres données relatives aux personnes concernées (pas même sur la base d'un pseudonyme, p. ex. un numéro de collaborateur). La mémoire doit être conçue de telle sorte que les données biométriques ne puissent ni être combinées avec d'autres informations, ni être lues dans le système pour être utilisées à d'autres fins.
- Le résultat du traitement des données ne doit contenir aucune donnée biométrique.

Usages interdits dans le domaine privé

Les usages suivants de systèmes de localisation de personnes sont interdits :

- La surveillance de personnes identifiables qui n'ont pas donné leur consentement. Aucun intérêt prépondérant n'est envisageable pour une telle surveillance. Une mesure de ce type serait illicite, car elle constituerait une violation des droits de la personnalité des personnes concernées.
- L'établissement de profils de la personnalité, y compris de profils de déplacement détaillés, sans le consentement explicite des personnes concernées. La législation accorde une protection élevée aux profils de la personnalité - tout comme aux données sensibles -, si bien qu'il est interdit d'en établir à l'insu des personnes concernées, sans leur consentement explicite. Qui plus est, aucun intérêt prépondérant n'est envisageable non plus dans ce cas de figure.
- La surveillance du personnel d'une entreprise. En vertu de l'art. 26 de l'ordonnance 3 relative à la loi sur le travail (hygiène, OLT 3), il est interdit d'utiliser des systèmes de surveillance ou de contrôle destinés à surveiller le comportement des travailleurs à leur poste de travail. C'est la raison pour laquelle une telle mesure serait illicite même si elle était prise moyennant le consentement des personnes concernées.

https://www.edoeb.admin.ch/content/edoeb/fr/home/protection-des-donnees/technologien/systemes-de-localisation-de-personnes.html