Groupe de travail «ARTICLE 29» sur la protection des données

881/11/FR
WP 185

Avis 13/2011 sur les services de géolocalisation des dispositifs mobiles intelligents

Adopté le 16 mai 2011

TABLE DES MATIERES

LE GROUPE DE TRAVAIL SUR LA PROTECTION DES PERSONNES À L'ÉGARD DU TRAITEMENT DES DONNÉES À CARACTÈRE PERSONNEL
institué par la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995,

vu les articles 29 et 30, paragraphe 1, point a), et paragraphe 3, de ladite directive,

vu son règlement intérieur,

A ADOPTE LE PRESENT DOCUMENT:

1. Introduction

Les informations géographiques jouent un rôle important dans notre société. La plupart des activités et décisions humaines ont une dimension géographique. Lorsque des informations sont liées à une position géographique, elles acquièrent généralement une plus grande valeur. Ces informations peuvent être de toutes sortes: financières, sanitaires ou autres données relatives au comportement du consommateur. En raison de la rapidité de l'évolution technologique des dispositifs mobiles intelligents associée à la généralisation de leur utilisation, une toute nouvelle catégorie de services basés sur la localisation se développe.

Le présent avis a pour objectif de clarifier le cadre juridique applicable aux services de géolocalisation proposés ou générés par les dispositifs mobiles intelligents capables de se connecter à l'internet et équipés de capteurs sensibles à la position tels que des systèmes de localisation GPS. Il peut notamment s'agir de services de cartographie et de navigation, de services géographiques personnalisés (y compris les points d'intérêt à proximité), de réalité augmentée, du géomarquage de contenu sur l'internet, de la possibilité de se tenir informé des allées et venues de ses amis, de la surveillance des enfants et de la publicité basée sur la localisation.

Le présent avis aborde également les trois principaux types d'infrastructure utilisés pour offrir des services de géolocalisation, à savoir le système GPS, les stations de base GSM et le système Wi-Fi. Une attention particulière est accordée à la nouvelle infrastructure basée sur la localisation de points d'accès Wi-Fi.

Le groupe de travail est bien conscient qu'il existe de nombreux autres services capables de traiter des données de localisation qui peuvent également susciter des inquiétudes en matière de protection des données. Il s'agit entre autres des systèmes de billetterie électronique, des systèmes de péage pour voitures et des services de navigation par satellite, du repérage de position à l'aide, par exemple, de caméras et de la géolocalisation d'adresses IP. Cependant, en raison de la rapidité de l'évolution technologique, notamment en matière de mappage de points d'accès sans fil, associée au fait que de nouveaux arrivants sur le marché se préparent à mettre au point de nouveaux services de localisation basés sur un mélange de données issues des stations de base et des systèmes GPS et Wi-Fi, le groupe de travail a décidé de clarifier de manière spécifique les conditions juridiques que doivent remplir ces services en vertu de la directive sur la protection des données.

Le présent avis commence par décrire les technologies concernées, puis identifie et évalue les risques d'atteinte à la vie privée, et enfin présente des conclusions concernant l'application des

articles juridiques pertinents à divers responsables du traitement qui recueillent et traitent les données de localisation provenant de dispositifs mobiles. Il s'agit, par exemple, des fournisseurs d'infrastructure de géolocalisation, des fabricants de téléphones intelligents et des développeurs d'applications basées sur la géolocalisation.

Le présent avis n'évaluera pas la technologie de géomarquage spécifique associée à ce que l'on appelle le Web 2.0, selon laquelle les utilisateurs intègrent des informations géoréférencées sur des réseaux sociaux tels que Facebook ou Twitter. Il ne rentrera pas non plus dans les détails de certaines autres technologies de géolocalisation qui sont utilisées pour interconnecter des dispositifs situés dans une zone relativement petite (centres commerciaux, aéroports, immeubles de bureaux, etc.), telles que les technologies Bluetooth, ZigBee, le gardiennage virtuel et les étiquettes RFID utilisant la technologie Wi-Fi, bien qu'une grande partie des conclusions du présent avis relatives au motif légitime, **à** l'information et aux droits des personnes concernées s'appliquent également à ces technologies lorsqu'elles servent à établir la position géographique de personnes par l'intermédiaire de leurs dispositifs.

2. Contexte: les différentes infrastructures de géolocalisation

2.1 Données des stations de base

La zone couverte par les différents opérateurs de télécommunications est divisée en zones communément appelées «cellules». Afin de pouvoir effectuer des appels téléphoniques ou se connecter à l'internet à l'aide du réseau 3G, le dispositif mobile doit se connecter à l'antenne (ci-après: la station de base) qui couvre cette cellule. Les cellules couvrent des zones de tailles différentes, ceci dépendant de l'interférence avec des montagnes ou de hauts bâtiments, par exemple.

Tant qu'un dispositif mobile est allumé, ce dernier est lié à une station de base particulière. L'opérateur de télécommunications enregistre continuellement ces liens. Chaque station de base possède un identifiant unique et est enregistrée en association avec une position spécifique. L'opérateur de télécommunications ainsi qu'un grand nombre de dispositifs mobiles eux-mêmes sont capables d'utiliser des signaux provenant de cellules se chevauchant (stations de base voisines) pour estimer la position du dispositif mobile avec une meilleure précision. Cette technique est également appelée triangulation.

Il est possible d'améliorer davantage la précision à l'aide d'informations telles que la puissance reçue d'un signal radio (RSSI), la différence entre les temps d'arrivée (TDOA), et l'angle d'incidence (AOA).

Les données des stations de base peuvent être utilisées de manière innovante, comme par exemple pour détecter des embouteillages. À chaque route correspond une vitesse moyenne pour chaque segment de la journée, mais lorsque les transferts à la station de base suivante prennent plus de temps que prévu, on peut supposer qu'il y a un embouteillage.

En résumé, ce procédé de positionnement permet d'obtenir rapidement une estimation approximative de localisation mais n'offre toutefois pas la précision des données GPS et Wi-Fi. La précision obtenue est d'environ 50 mètres dans des zones urbaines densément peuplées, mais peut être de plusieurs kilomètres en zone rurale.

2.2 La technologie GPS

Les dispositifs mobiles intelligents comportent un jeu de puces incorporé doté d'un récepteur GPS permettant de les localiser.

La technologie GPS (Global Positioning System) utilise 31 satellites tournant chacun dans l'une des 6 différentes orbites autour de la terre[1]. Chaque satellite transmet un signal radio très précis.

Le dispositif mobile peut déterminer sa position lorsque le capteur GPS capture au moins 4 de ces signaux. À la différence des données de stations de base, le signal n'est émis que dans un seul sens. Les entités qui gèrent les satellites ne peuvent pas suivre les appareils qui ont reçu le signal radio.

La technologie GPS permet une localisation précise, entre 4 et 15 mètres. Le principal inconvénient du système GPS est que le démarrage est relativement lent[2]. Un autre inconvénient est qu'il fonctionne mal voire pas du tout en intérieur. Dans la pratique, la technologie GPS est donc souvent utilisée en association avec des données de stations de base et/ou des points d'accès Wi-Fi mappés.

2.3 La technologie Wi-Fi

2.3.1 Points d'accès Wi-Fi

Les points d'accès Wi-Fi sont utilisés depuis peu comme source d'informations de géolocalisation. La technologie utilisée est similaire à celle des stations de base. Les deux types de technologies se basent sur un identifiant unique (appartenant à la station de base ou au point d'accès Wi-Fi) qui peut être détecté par un dispositif mobile, puis envoyé à un service comportant un emplacement pour chaque identifiant unique.

L'identifiant unique attribué à chaque point d'accès Wi-Fi correspond à son adresse MAC. Une adresse MAC est un identifiant unique attribué à une interface réseau et qui est généralement enregistré sur des composants matériels tels que des puces de mémoire et/ou des cartes d'interface réseau d'ordinateurs, de téléphones, d'ordinateurs portables ou de points d'accès. [3]

La raison pour laquelle les points d'accès Wi-Fi peuvent être utilisés comme source d'informations de géolocalisation est qu'ils signalent constamment leur existence. La plupart des points d'accès à l'internet à large bande sont également munis d'une antenne Wi-Fi par défaut. Sur la plupart des points d'accès les plus couramment utilisés en Europe, la connexion est «activée» par défaut, même si l'utilisateur a connecté son ou ses ordinateurs au point d'accès à l'aide de câbles physiques. Tout comme une radio, le point d'accès Wi-Fi transmet continuellement son propre nom réseau et son adresse MAC, même si personne n'utilise la

---

1 Le système de positionnement global est constitué de satellites lancés par les États-Unis d'Amérique à des fins militaires. La Commission européenne prévoit de lancer, d'ici 2014, Galileo, un réseau de 18 satellites procurant gratuitement un service de positionnement global par satellite à usage non militaire. Les deux premiers satellites devraient être lancés en 2011, et deux autres en 2012. Source: Commission européenne, «Commission presents midterm review of Galileo and EGNOS», 25 Janvier 2011, URL: http://ec.europa.eu/enterprise/newsroom/cf/itemlongdetail.cfm?displayType=news&tpa_id=0&item_id=4835

2 Afin d'accélérer la détection initiale du signal GPS, il est possible de préinstaller ce que l'on appelle des «tables arc-en-ciel» contenant le positionnement escompté des différents satellites au cours des prochaines semaines.

3 Un exemple d'adresse MAC est: 00-1F-3F-D7-3C-58. L'adresse MAC d'un point d'accès Wi-Fi est appelée BSSID (Basic Service Set Identifier).

connexion et même dans le cas où les contenus de la communication sans fil sont chiffrés à l'aide du système WEP, WPA ou WPA2.

Il existe deux manières différentes de recueillir les adresses MAC de points d'accès WI-FI[4].

1. Le balayage actif: il consiste à envoyer des requêtes actives[5] à tous les points d'accès Wi-Fi avoisinants et à enregistrer les réponses. Ces réponses n'incluent pas les informations concernant des dispositifs connectés au point d'accès Wi-Fi.

2. Le balayage passif: il consiste à enregistrer les trames de balises périodiques transmises par chaque point d'accès (habituellement à raison de 10 fois par seconde). Une alternative non standard consiste en ce que des outils enregistrent plus largement toutes les trames Wi-Fi transmises par les points d'accès, dont celles qui ne diffusent pas de signaux de balise. Si ce type de balayage est effectué sans que les principes de respect de la vie privée soient pris en compte dès la conception, il peut mener à la collecte des données échangées entre les points d'accès et les dispositifs qui y sont
rattachés. De cette manière, il serait possible d'enregistrer les adresses MAC des ordinateurs de bureau, des ordinateurs portables et des imprimantes. Ce type de balayage pourrait également entraîner l'enregistrement illicite du contenu des communications. Ce contenu peut être extrait facilement si le chiffrement Wi-Fi (WEP/WPA/WPA2) n'est pas activé sur le point d'accès Wi-Fi.

Il est possible de calculer la position d'un point d'accès Wi-Fi de deux manières différentes.

1. Statiquement/une seule fois: les responsables du traitement eux-mêmes recueillent les adresses MAC de points d'accès Wi-Fi en circulant dans des véhicules équipés d'une antenne. Ils enregistrent la latitude/longitude du véhicule à l'instant où le signal est capturé, ce qui leur permet de calculer la position des points d'accès, en fonction, entre autres, de l'intensité de signal.

2. Dynamiquement/en continu: les utilisateurs de services de géolocalisation recueillent automatiquement les adresses IP captées par leurs appareils Wi-Fi lorsqu'ils utilisent par exemple une carte en ligne pour déterminer leur propre position (Où suis-je?). Le dispositif mobile envoie alors toutes les informations disponibles au fournisseur de services de géolocalisation, dont les adresses MAC, les identifiants SSID et l'intensité du signal. Le responsable du traitement peut utiliser ces observations continues afin de calculer et/ou d'améliorer les positions des points d'accès Wi-Fi contenus dans sa base de données avec des points d'accès Wi-Fi mappés.

Il est important de noter que les dispositifs mobiles n'ont pas besoin de se «connecter» à des points d'accès Wi-Fi pour recueillir des informations Wi-Fi. Ils détectent automatiquement la présence de points d'accès (en mode balayage actif ou passif) et recueillent automatiquement des données les concernant.

De plus, les téléphones mobiles demandant l'établissement de leur position géographique enverront non seulement des données Wi-Fi, mais aussi fréquemment d'autres informations de

[4] Les systèmes de balayage actif et passif ont été normalisés par l'IEEE 802.11 afin de détecter les points d'accès.

[5] Afin de recueillir des adresses MAC, le responsable du traitement envoie une trame de requête («probe request») à tous les points d'accès.

localisation qu'ils détiennent, dont des données GPS et des données de stations de base. Ceci permet au fournisseur de calculer la position de «nouveaux» points d'accès Wi-Fi et/ou d'améliorer les positions des points d'accès Wi-Fi qui étaient déjà inclus dans la base de données. De cette manière, la collecte d'informations concernant les points d'accès Wi-Fi est décentralisée d'une manière très efficace, sans que les clients n'en soient nécessairement conscients.

En résumé, la géolocalisation basée sur les points d'accès Wi-Fi procure une localisation rapide et, grâce à des mesures effectuées en continu, de plus en plus précise.

3. Risques d'atteinte à la vie privée

Un dispositif mobile intelligent est très intimement lié une personne donnée. La plupart des personnes gardent généralement leurs dispositifs mobiles, à proximité immédiate, que ce soit dans leur poche ou leur sac, ou même sur leur table de chevet à côté du lit.

Il est rare que l'on prête un appareil de ce genre à une autre personne. La plupart des gens sont conscients que leur dispositif mobile contient tout un éventail d'informations extrêmement intimes pouvant aller de leurs courriers électroniques à des photos privées, en passant par leur historique de navigation et leur liste de contacts, par exemple.

Cela permet aux fournisseurs de services basés sur la géolocalisation d'obtenir une vision intime des habitudes et des schémas de comportement du propriétaire d'un tel appareil et d'établir des profils très détaillés. À partir d'un schéma d'inactivité la nuit, il est possible de déduire le lieu où dort le propriétaire, et à partir d'un schéma de trajets réguliers effectués le matin, de connaître la position d'un employeur. Le schéma peut également inclure des données issues des schémas de déplacement d'amis, sur la base de ce que l'on appelle le «*graphique social*[6]»

Un schéma de comportement peut également inclure des *catégories spéciales de données*, dans le cas, par exemple, où elles révèlent des visites à des hôpitaux ou à des lieux de culte, la présence à des manifestations politiques ou à d'autres lieux spécifiques révélant des informations concernant la vie sexuelle par exemple. Ces profils peuvent être utilisés pour prendre des décisions pouvant affecter le propriétaire de manière significative.

La technologie des dispositifs mobiles intelligents permet une surveillance constante de données de localisation. Les téléphones intelligents peuvent collecter en permanence des signaux de stations de base et de points d'accès Wi-Fi. Sur le plan technique, la surveillance peut se faire en secret, sans en informer le propriétaire. Elle peut également se faire de manière semi secrète, lorsque les personnes «oublient» que le paramètre des services de localisation est «activé» ou n'en sont pas correctement informées, ou lorsque les paramètres d'accessibilité des données de localisation passent de «privé» à «public».

Même lorsque les gens rendent intentionnellement leurs données de géolocalisation disponibles sur l'internet, par l'intermédiaire de services de géomarquage, l'accessibilité illimitée de ces données au niveau mondial crée de nouveaux risques (vol de données, cambriolage, voire agression physique ou harcèlement).

---

[6] Le «graphe social» se refère à la visibilité d'amis sur les sites de réseaux sociaux et à la capacité de déduire des traits de comportement à partir de données concernant ces amis.

Comme dans le cas d'autres nouvelles technologies, le risque le plus important que comporte l'utilisation de données de localisation est le détournement d'usage, c'est-à-dire le fait que de nouvelles finalités, qui n'étaient pas prévues au moment de la collecte initiale des données, soient visées à mesure que de nouveaux types d'informations deviennent disponibles.

4. Cadre juridique

Le cadre juridique concerné est la directive sur la protection des données (95/46/CE). Il s'applique à chaque fois que des données à caractère personnel sont traitées suite au traitement de données de localisation. La directive vie privée et communications électroniques (2002/58/CE, telle que modifiée par la directive 2009/136/CE) s'applique uniquement au traitement des données de stations de base par les services et réseaux de communications électroniques publics (opérateurs de télécommunications).

4.1 Données de stations de base traitées par les opérateurs de télécommunications

Les opérateurs de télécommunications traitent continuellement des données de stations de base dans le cadre de la fourniture de services de communications électroniques publics[7]. Ils peuvent également traiter des données de stations de base afin d'offrir des services à valeur ajoutée. Ce cas a déjà été abordé par le groupe de travail dans l'avis 5/2005 (WP115). Bien que certains des exemples contenus dans l'avis soient inévitablement devenus caducs du fait que les appareils munis de capteurs et de technologies internet deviennent sans cesse plus petits, les conclusions et recommandations juridiques restent valables à l'égard de l'utilisation des données de stations de base.

1. Étant donné que les données de localisation issues des stations de base se rapportent à une personne physique identifiée ou identifiable, elles sont soumises aux dispositions sur la protection des données à caractère personnel prévues dans la directive 95/46/CE du 24 Octobre 1995.
2. La directive 2002/58/CE du 12 Juillet 2002 (telle que modifiée en novembre 2009 par la directive 2009/136/CE) est également applicable, selon la définition donnée à l'article 2, point c) de cette directive:
   «données de localisation»: toutes les données traitées dans un réseau de communications électroniques ou par un service de communications électroniques indiquant la position géographique de l'équipement terminal d'un utilisateur d'un service de communications électroniques accessible au public;

Si un opérateur de télécommunications offre un service de géolocalisation hybride, qui se base également sur le traitement d'autres types de données de localisation telles que des données GPS ou Wi-Fi, cette activité est considérée comme un service de communications électroniques public. L'opérateur de télécommunications doit obtenir le consentement préalable de ses clients s'il fournit ces données de géolocalisation à un tiers.

[7] Il convient de noter que la fourniture de hotspots Wi-Fi publics par des fournisseurs de télécommunications peut également être considérée comme un service de communications électroniques public et devrait donc principalement se conformer aux dispositions de la directive vie privée et communications électroniques.

4.2 Données de stations de base, Wi-Fi et GPS traitées par des prestataires de services de la société de l'information

4.2.1 Applicabilité de la directive vie privée et communications électroniques révisée

En règle générale, les sociétés qui fournissent des services et des applications de localisation sur la base d'une combinaison de données de stations de base, GPS et Wi-Fi sont des *services de la société de l'information.* À ce titre, elles sont explicitement exclues de la directive vie privée et communications électroniques, d'après la stricte définition du service de communications électroniques au point c) de l'article 2 de la directive-cadre révisée (non modifiée) [8].

La directive vie privée et communications électroniques ne s'applique pas au traitement des données de localisation par les services de la société de l'information, même lorsqu'un tel traitement est effectué par l'intermédiaire d'un réseau de communications électroniques public. Un utilisateur peut choisir de transmettre des données GPS sur l'internet, lorsqu'il accède à des services de navigation sur l'internet, par exemple. Dans ce cas, le signal GPS est transmis au niveau «application» de la communication internet, indépendamment du réseau GSM. Le fournisseur de services de télécommunications joue simplement le rôle de transmetteur. Il ne peut pas accéder aux données GPS/ et/ou Wi-Fi et/ou de stations de base communiquées échangées entre le dispositif mobile intelligent d'un utilisateur/abonné et un service de la société de l'information, à moins d'utiliser des moyens très intrusifs tels que le «*deep packet inspection*».

4.2.2 Applicabilité de la directive sur la protection de la vie privée

Là où la directive vie privée et communications électroniques ne s'applique pas, la directive 95/46/CE s'applique selon l'article 1er, paragraphe 2:

«Les dispositions de la présente directive précisent et complètent la directive 95/46/CE aux fins énoncées au paragraphe 1.»

D'après la directive sur la protection des données, on entend par données à caractère personnel *toute information concernant une personne physique identifiée ou identifiable (personne concernée); est réputée identifiable une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale* – article 2 de la directive.

Le considérant 26 de ladite directive accorde une attention particulière au terme «identifiable» lorsqu'il énonce que «[considérant] que, pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens susceptibles d'être raisonnablement mis en œuvre, soit par le responsable du traitement, soit par une autre personne, pour identifier ladite personne;».

---

[8] Directive 2002/21/CE du 7 mars 2002, article 2, point c): *«service de communications électroniques»: le service fourni normalement contre rémunération qui consiste entièrement ou principalement en la transmission de signaux sur des réseaux de communications électroniques, y compris les services de télécommunications et les services de transmission sur les réseaux utilisés pour la radiodiffusion, mais qui exclut les services consistant à fournir des contenus à l'aide de réseaux et de services de communications électroniques ou à exercer une responsabilité éditoriale sur ces contenus; il ne comprend pas les services de la société de l'information tels que définis à l'article 1er de la directive 98/34/CE qui ne consistent pas entièrement ou principalement en la transmission de signaux sur des réseaux de communications électroniques;*

Le considérant 27 de la directive expose les grandes lignes du vaste champ d'application de la protection: «[considérant] *que le champ de cette protection ne doit pas en effet dépendre des techniques utilisées, sauf à créer de graves risques de détournement*;».

Le groupe de travail a fourni des orientations détaillées quant à la définition des données à caractère personnel dans son avis 4/2007 sur le concept de données à caractère personnel.

Dispositifs mobiles intelligents
Les dispositifs mobiles intelligents sont inextricablement liés aux personnes physiques. Il est habituellement possible de les identifier directement et indirectement.

Premièrement, l'opérateur de télécommunications fournissant un accès à l'internet mobile et par GSM possède généralement un registre comportant le nom, l'adresse, et les coordonnées bancaires de chaque client, auxquels sont associés plusieurs numéros uniques du dispositif, tels que les numéros «IMEI» (identité internationale de l'équipement mobile) et «IMSI» (identité internationale de l'abonné mobile)

Deuxièmement, l'achat de logiciels supplémentaires pour le dispositif (applications ou «apps») nécessite généralement un numéro de carte de crédit, des données d'identification directe venant ainsi s'ajouter à la combinaison du ou des numéros uniques et des données de localisation.

L'identification indirecte peut s'obtenir par l'intermédiaire de la combinaison du ou des numéros uniques du dispositif et d'une ou de plusieurs positions calculées.

Chaque dispositif mobile intelligent possède au moins un identifiant unique, à savoir l'adresse MAC. Le dispositif peut posséder d'autres numéros d'identification uniques, ajoutés par le développeur du système d'exploitation. Ces identifiants peuvent être transmis et traités ultérieurement dans le contexte de services de géolocalisation. Il est évident que la position d'un dispositif donné peut être calculée d'une manière très précise, surtout lorsque les différentes infrastructures de géolocalisation sont combinées. Cette localisation peut indiquer une maison ou un employeur. Il est notamment possible d'identifier le propriétaire du dispositif grâce à des observations répétées.

En analysant les moyens d'identification disponibles, il faut tenir compte du fait que les gens ont tendance à divulguer de plus en plus de données de localisation à caractère personnel sur l'internet, par exemple en publiant l'emplacement de leur maison ou de leur lieu de travail en combinaison avec d'autres données d'identification. Une telle divulgation de données peut également se faire à leur insu, lorsqu'ils font l'objet d'un géomarquage par d'autres personnes. Le lien peut ainsi être aisément établi entre un emplacement ou un schéma de comportement et une personne donnée.

De plus, d'après l'avis 4/2007 sur le concept de données à caractère personnel, il convient également de noter que l'attribution d'un identifiant unique, dans le contexte décrit ci-dessus, permet de repérer un utilisateur d'un dispositif spécifique, et donc de l'«isoler», même si son véritable nom n'est pas connu.

Points d'accès Wi-Fi
L'identification indirecte s'applique également aux points d'accès Wi-Fi[9]. L'adresse MAC d'un point d'accès Wi-Fi, lorsqu'elle est associée à sa position calculée, est inextricablement liée à la position du propriétaire du point d'accès.

Un responsable du traitement correctement équipé peut calculer la position d'un point d'accès Wi-Fi avec une précision de plus en plus grande en fonction de l'intensité de signal et des mises à jour régulières de la position par l'intermédiaire des utilisateurs de son service de géolocalisation.

À l'aide de ces ressources, il est possible d'identifier dans de nombreux cas le petit groupe d'appartements ou de maisons où vit le propriétaire du point d'accès. La facilité avec laquelle il est possible d'identifier ce propriétaire à partir de l'adresse MAC va dépendre de l'environnement:

- Dans des zones faiblement peuplées, dans lesquelles l'adresse MAC désigne une maison individuelle, le propriétaire de la résidence peut être déterminé directement à l'aide d'outils comme des registres de propriétaires, des annuaires de pages blanches, des listes électorales ou simplement un moteur de recherche[10].
- Dans des zones plus fortement peuplées, à l'aide de ressources comme l'intensité de signal et/ou les identifiants SSID (pouvant être détectés par quiconque possède un appareil Wi-Fi), il est possible de déterminer avec précision la position du point d'accès et ainsi, dans de nombreux cas, de déterminer l'identité de la ou des personnes vivant à l'endroit précis (maison ou appartement) où se trouve le point d'accès.
- Dans des zones très fortement peuplées, même à l'aide d'informations sur l'intensité de signal, la position possible du point d'accès qu'indiquera l'adresse MAC correspondra à plusieurs appartements Dans ces circonstances, il n'est pas possible, sans efforts déraisonnables, de déterminer avec précision l'identité de la personne vivant dans l'appartement où se trouve le point d'accès.

Le fait qu'à l'heure actuelle, dans certains cas, le propriétaire du dispositif ne peut pas être identifié à moins d'employer des moyens extrêmes ne compromet pas la conclusion générale selon laquelle la combinaison d'une adresse MAC d'un point d'accès Wi-Fi et de sa position calculée devrait être traitée de la même manière que des données à caractère personnel.

Dans ces conditions et compte tenu du fait qu'il est peu probable que le responsable du traitement des données fasse la distinction entre les cas où le propriétaire du point d'accès Wi-Fi est identifiable et les cas où il ne l'est pas, le responsable du traitement des données devrait traiter toutes les données concernant les routeurs Wi-Fi comme des données à caractère personnel.

Il est important de rappeler qu'il n'est pas nécessaire que la finalité du traitement de ces données de géolocalisation soit d'identifier les utilisateurs. L'intensité des efforts requis pour identifier les propriétaires des points d'accès Wi-Fi dépend fortement des moyens techniques dont dispose le responsable du traitement ou toute autre personne pour identifier lesdits propriétaires.

---

[9] Les points d'accès Wi-Fi peuvent même être identifiables directement, si le fournisseur d'accès à l'internet conserve un registre des adresses MAC des routeurs Wi-Fi qu'il fournit à ses clients identifiés.

[10] La disponibilité de tels registres ou annuaires varie selon l'État membre.

5. Obligations découlant de la législation sur la protection des données

5.1 Responsable du traitement des données

Dans le contexte des services de géolocalisation en ligne que procurent les services de la société de l'information, on distingue trois fonctions différentes, auxquelles sont associées des responsabilités distinctes en matière de traitement des données à caractère personnel. Il s'agit du responsable d'une infrastructure de géolocalisation; du fournisseur d'application ou de service de géolocalisation spécifique et du développeur du système d'exploitation d'un dispositif mobile intelligent. En pratique, les sociétés endossent souvent de nombreux rôles en même temps, par exemple lorsqu'elles combinent un système d'exploitation doté d'une base de données comprenant des points d'accès Wi-Fi mappés et une plate-forme publicitaire.

5.1.1 Responsables d'infrastructure de géolocalisation

Tout comme le font les opérateurs de télécommunications lorsqu'ils traitent la position d'un dispositif spécifique à l'aide de leurs stations de base, les propriétaires de bases de données comprenant des points d'accès Wi-Fi mappés traitent des données à caractère personnel lorsqu'ils calculent la position d'un dispositif mobile intelligent spécifique. Étant donné que les opérateurs et les propriétaires déterminent les finalités et modalités de ce traitement, ils sont considérés comme des responsables du traitement au sens de l'article 2, point d), de la directive sur la protection des données.

Il est important de souligner que le dispositif spécifique contribue à calculer sa position en transmettant au propriétaire de la base de données ses propres données de localisation (la plupart du temps une combinaison de données GPS, Wi-Fi et de stations de base) et les identifiants uniques des points d'accès Wi-Fi à proximité immédiate[11]. Un tel dispositif répond également au critère de l'article 4.1, point c) de la directive sur la protection des données, *moyens situés sur le territoire d'un État membre.*

Étant donné que l'adresse MAC d'un point d'accès Wi-Fi, combinée à sa position calculée, devrait être considérée de la même manière que des données à caractère personnel, la collecte de ces données entraîne également le traitement de données à caractère personnel. Quelle que soit la manière dont ces données sont collectées (une seule fois ou régulièrement), le propriétaire d'une telle base de données doit se conformer aux obligations découlant de la directive sur la protection des données.

5.1.2 Fournisseurs d'applications et de services de géolocalisation

Les dispositifs mobiles intelligents permettent l'installation de logiciels de tiers, appelés *«applications»*. De telles applications peuvent traiter les données de localisation (et autres données) d'un dispositif mobile intelligent indépendamment du développeur du système d'exploitation et/ou des responsables d'infrastructure de géolocalisation.

Comme exemples de tels services, on citera un service météorologique qui prévoit les risques de pluie dans les prochaines heures dans une région très spécifique, un service qui procure des informations sur les commerces à proximité, un service d'identification de téléphone égaré ou un service qui indique à l'utilisateur l'emplacement de ses amis.

---

[11] Le dispositif mobile peut transmettre les diverses données de géolocalisation qu'il reçoit au responsable du traitement qui calculera sa position, ou calculer sa position lui-même. Dans les deux cas, le dispositif consitue un équipement essentiel au traitement.

Le fournisseur d’une application capable de traiter des données de géolocalisation est le responsable du traitement de données à caractère personnel résultant de l’installation et de l’utilisation de l’application.

Il n’est évidemment pas nécessaire de toujours installer un logiciel séparé sur un dispositif mobile intelligent. Il est également possible d’accéder à de nombreux services de géolocalisation par l’intermédiaire d’un navigateur. Un service de ce genre peut par exemple consister en l’utilisation d’une carte en ligne pour guider une personne se déplaçant à pied dans une ville.

5.1.3 Développeur du système d’exploitation

Le développeur du système d’exploitation du dispositif mobile intelligent peut être un responsable du traitement des données de géolocalisation lorsqu’il est directement en interaction avec l’utilisateur et recueille des données à caractère personnel (en demandant un enregistrement initial de l’utilisateur et/ou en recueillant des informations de localisation aux fins de l’amélioration des services). En tant que responsable du traitement, le développeur doit appliquer les principes de la prise en compte du respect de la vie privée dès la conception pour éviter la surveillance secrète, soit par le dispositif lui-même, soit par les différents services et applications.

Un développeur est également le responsable du traitement des données qu'il détient si le dispositif possède une fonctionnalité «phone home» au moyen de laquelle il transmet des informations sur le lieu où il se trouve. Étant donné que dans ce cas le développeur décide des modalités et finalités de ce transfert de données, il est le responsable du traitement de ces données. Un exemple courant d’une telle fonctionnalité «phone home» est la mise à jour automatique du fuseau horaire en fonction de l’emplacement.

Troisièmement, le développeur est responsable du traitement lorsqu’il offre une plate-forme publicitaire et/ou un environnement de type «magasin en ligne» pour la vente d'applications et qu’il est capable de traiter des données à caractère personnel résultant (de l’installation et de l’utilisation) des applications de géolocalisation, indépendamment des fournisseurs d’application.

5.2 Responsabilités des autres parties

Il existe bien d’autres parties en ligne qui permettent de traiter (ultérieurement) des données de localisation, telles que les navigateurs, les sites de socialisation ou les supports de communication qui permettent le «géomarquage» par exemple. Lorsqu’elles intègrent des fonctions de géolocalisation dans leur plate-forme, ces parties ont une grande part de responsabilité dans la définition des paramètres par défaut de l’application (activation ou désactivation par défaut). Bien qu’elles ne soient des responsables du traitement que dans la mesure où elles traitent elles-mêmes des données à caractère personnel de manière active, ces parties ont un rôle essentiel à jouer pour garantir le caractère légitime du traitement de données effectué par des responsables du traitement tels que les fournisseurs d’applications spécifiques, par exemple lorsqu’il s’agit de la visibilité et de la qualité des informations concernant le traitement des données de géolocalisation.

5.3 Motif légitime

5.3.1 Dispositifs mobiles intelligents

Si des opérateurs de télécommunications veulent utiliser des données de stations de base afin de fournir un service à valeur ajoutée à un client, conformément à la directive vie privée et communications électroniques révisée, ils doivent obtenir le consentement préalable du client. Ils doivent également s'assurer que le client est informé des modalités de ce traitement.

Étant donné le caractère sensible du traitement de (schémas de) données de localisation, le *consentement préalable en connaissance de cause* est également le principal motif conférant un caractère légitime au traitement de données quand il s'agit du traitement des emplacements d'un dispositif mobile intelligent dans le contexte des services de la société de l'information.

Conformément à la directive sur la protection des données, article 2, point h), le consentement doit être une manifestation de volonté, libre, spécifique et informée des souhaits de la personne concernée.

En fonction du type de technologie utilisée, le dispositif de l'utilisateur joue un rôle relativement actif dans le traitement des données de géolocalisation. Le dispositif est capable de transmettre des données de localisation de différentes sources à des tiers. L'existence de cette capacité technique ne signifie pas qu'un tel traitement de données est automatiquement légal. Dans le cas où les paramètres par défaut d'un système d'exploitation permettraient la transmission de données de localisation, une absence d'intervention de la part des utilisateurs ne devrait pas être assimilée à un libre consentement de ces derniers.

Dans la mesure où les développeurs de systèmes d'exploitation et d'autres services de la société de l'information traitent eux-mêmes activement des données de géolocalisation (par exemple lorsqu'ils obtiennent des informations de localisation à partir du dispositif ou par son intermédiaire), ils doivent également chercher à obtenir le consentement préalable en connaissance de cause des utilisateurs. Il convient de préciser qu'un tel consentement ne peut pas être obtenu librement en obligeant les utilisateurs à accepter les conditions générales, ni en leur proposant des possibilités de non-participation. Par défaut, les services de localisation devraient être désactivés, et les utilisateurs devraient pouvoir choisir de les activer pour certaines applications spécifiques.

Consentement des travailleurs

Le consentement en tant que motif légitime de traitement est problématique dans le contexte professionnel. Le groupe de travail, dans son avis sur le traitement des données à caractère personnel dans le contexte professionnel a écrit: «*si le consentement du travailleur est nécessaire et que l'absence de consentement peut entraîner un préjudice réel ou potentiel pour le travailleur, le consentement n'est pas valable au titre de l'article 7 ou de l'article 8, dans la mesure où il n'est pas donné librement. Si le travailleur n'a pas la possibilité de refuser, il ne s'agit pas de consentement.* (…) *Une pierre d'achoppement peut exister si le consentement est une condition d'emploi. Le travailleur peut, en théorie, refuser de donner son consentement, mais il peut perdre alors une opportunité d'emploi. Dans ces circonstances, le consentement n'étant pas donné librement, n'est donc pas valable*»[12]. Au lieu de chercher à obtenir le consentement, les employeurs devraient déterminer s'il est possible de prouver la nécessité de

[12] WP48, avis 8/2001 sur le traitement des données à caractère personnel dans le contexte professionnel.

surveiller l'emplacement exact des travailleurs pour une finalité légitime et mettre en balance cette nécessité avec les droits et libertés fondamentaux des travailleurs. Dans le cas où la nécessité peut être dûment justifiée, la base juridique d'un tel traitement pourrait se fonder sur l'intérêt légitime du responsable du traitement [article 7, point f) de la directive sur la protection des données]. L'employeur doit toujours rechercher le moyen le moins intrusif, éviter une surveillance continuelle et par exemple choisir un système qui envoie une alerte lorsqu'un travailleur traverse une frontière virtuelle définie au préalable. Un travailleur doit pouvoir éteindre tout appareil de surveillance en dehors des heures de travail et la manière de le faire doit lui être expliquée. Les dispositifs de surveillance des véhicules ne sont pas des dispositifs de surveillance du personnel. Leur fonction est de repérer ou de contrôler la position des véhicules dans lesquels ils sont installés. Les employeurs ne devraient pas les considérer comme des dispositifs leur permettant de repérer ou contrôler le comportement ou les allées et venues de chauffeurs ou autres membres du personnel, par exemple en envoyant des alertes en rapport avec la vitesse du véhicule.

Consentement des enfants

Dans certains cas, le consentement des enfants doit être donné par les parents ou autres représentants légaux. Cela implique par exemple que le fournisseur d'une application de géolocalisation doit notifier les parents de la collecte et de l'utilisation de données de géolocalisation concernant leurs enfants et obtenir leur consentement avant de recueillir et d'utiliser ultérieurement les informations concernant leurs enfants. Certaines applications de géolocalisation sont spécifiquement conçues pour la surveillance parentale, par exemple en révélant en permanence la position du dispositif sur un site Web, ou en émettant une alerte si l'appareil quitte un territoire délimité au préalable. L'utilisation de telles applications pose problème. Le groupe de travail «article 29», dans son avis 2/2009[13] sur la protection de données d'enfants à caractère personnel, a écrit*: Il ne devrait jamais arriver que, pour des raisons de sécurité, les enfants soient confrontés à une surveillance excessive limitant leur autonomie. Dans ce contexte, un équilibre doit être trouvé entre la protection de l'intimité et de la vie privée des enfants, et leur sécurité.*

Le cadre juridique prévoit que les parents sont responsables de la protection du droit à la vie privée de leurs enfants. Pour le moins, si les parents estiment que l'utilisation d'une telle application est justifiée dans des circonstances spécifiques, les enfants doivent en être informés et doivent pouvoir participer, dès que cela s'avère raisonnablement possible, à la décision d'utiliser une telle application.

Le consentement doit être spécifique, pour chacune des différentes finalités pour lesquelles les données sont traitées. Le responsable du traitement doit faire savoir de manière très claire si son service se limite à donner une réponse à la question volontaire «Où suis-je en ce moment précis?», ou si son objectif est de créer des réponses aux questions «Où êtes-vous, où avez-vous été et où serez-vous la semaine prochaine?». En d'autres termes, le responsable du traitement doit accorder une attention particulière au consentement donné pour des finalités auxquelles la personne concernée n'est pas préparée, comme par exemple pour l'établissement de profils et/ou le ciblage comportemental.

Si les finalités du traitement changent de manière significative, le responsable du traitement doit solliciter une nouvelle fois le consentement spécifique. Par exemple, s'il a été initialement

[13] WP160, Avis 2/2009 sur la protection des données à caractère personnel de l'enfant (Principes généraux et cas particulier des écoles).

mentionné par une société qu'elle ne partagerait pas de données à caractère personnel avec une autre société, mais qu'elle souhaite à présent les partager, elle doit solliciter activement le consentement préalable de chaque client. Une absence de réponse (ou tout autre type de scénario de non-participation) ne suffit pas.

Il est important d'effectuer une distinction entre le consentement donné pour un service ponctuel et celui donné dans le cadre d'un abonnement régulier. Par exemple, afin d'utiliser un service de géolocalisation spécifique, il peut être nécessaire d'activer les services de géolocalisation du dispositif ou du navigateur. Si cette fonctionnalité de géolocalisation est activée, les sites Web peuvent tous lire les informations de localisation de l'utilisateur de ce dispositif mobile intelligent. Afin de prévenir les risques de surveillance secrète, le groupe de travail «article 29» considère qu'il est essentiel que le dispositif avertisse continuellement l'utilisateur que la géolocalisation est activée, par exemple par l'intermédiaire d'une icône visible en permanence.

Le groupe de travail recommande aux fournisseurs d'applications ou de services de géolocalisation de solliciter une nouvelle fois le consentement de la personne (même lorsqu'aucune modification n'a été apportée à la nature du traitement) après un délai approprié. Par exemple, il y aurait lieu de cesser de traiter les données de localisation dans le cas où une personne n'aurait pas activement utilisé le service au cours des 12 derniers mois. Même dans le cas où le service est utilisé, la nature du traitement de ses données à caractère personnel doit lui être rappelée au moins une fois par an (ou plus souvent si la nature du traitement le justifie) et un moyen de renoncer facilement à participer au traitement de données doit lui être proposé.

Enfin, la personne concernée doit surtout pouvoir retirer son consentement très facilement, sans aucun effet négatif sur l'utilisation de son appareil. Indépendamment des directives européennes sur la protection des données, le World Wide Web Consortium (W3C) a élaboré un projet de norme pour l'API de géolocalisation qui souligne la nécessité d'un consentement préalable, libre, exprès et éclairé[14]. Le W3C explique notamment la nécessité de respecter le retrait du consentement, en conseillant aux personnes chargées de la mise en œuvre de la norme de considérer que «*le contenu hébergé à une adresse URL donnée évolue de telle façon que les autorisations de localisation déjà accordées ne s'appliquent plus en ce qui concerne l'utilisateur. Ou alors, les utilisateurs auront simplement changé d'avis.*»

Exemple de meilleure pratique pour les fournisseurs d'applications de géolocalisation

Une application qui souhaite utiliser des données de géolocalisation informe clairement l'utilisateur des raisons pour lesquelles elle souhaite utiliser les données, et demande un consentement sans équivoque pour chacune de ces raisons qui peuvent différer les unes des autres. L'utilisateur choisit activement le niveau de granularité de géolocalisation (par exemple à l'échelle d'un pays, d'une ville, d'un code postal, ou à l'échelle la plus précise possible). Une fois que le service de localisation est activé, une icône indiquant que les services de localisation sont activés est visible en permanence sur chaque écran. L'utilisateur peut retirer son consentement à tout moment, sans avoir à quitter l'application. L'utilisateur est également en mesure de supprimer facilement et de manière définitive toute donnée de localisation stockée sur le dispositif.

[14] API de géolocalisation du W3C: http://www.w3.org/TR/geolocation-API/

5.3.2 Points d'accès Wi-Fi

Sur la base de la directive sur la protection des données, les sociétés peuvent avoir un intérêt légitime à recueillir et à traiter les adresses MAC et les positions calculées de points d'accès Wi-Fi dans le but spécifique d'offrir des services de géolocalisation.

Le motif légitime de l'article 7, point f) de la directive sur la protection des données requiert un équilibre entre les intérêts légitimes du responsable du traitement et les droits fondamentaux des personnes concernées. Étant donné la nature semi statique des points d'accès Wi-Fi, le mappage de points d'accès Wi-Fi représente en principe une menace moins grande à l'égard de la vie privée des propriétaires de ces points d'accès que celle du repérage en temps réel des positions de dispositifs mobiles intelligents.

L'équilibre à trouver entre les droits du responsable du traitement et les droits de la personne concernée est dynamique. Afin que les responsables du traitement réussissent à laisser leurs intérêts légitimes prévaloir avec le temps sur les intérêts des personnes concernées, ils doivent élaborer et mettre en œuvre des garanties, comme le droit de renoncer facilement et de façon définitive à participer à la base de données, sans avoir à fournir de données à caractère personnel supplémentaires au responsable du traitement d'une telle base de données. Ils peuvent par exemple utiliser un logiciel pour détecter automatiquement qu'une personne est connectée à un point d'accès spécifique[15].

De plus, la collecte et le traitement d'identifiants SSID ne sont pas nécessaires pour pouvoir offrir des services de géolocalisation. Par conséquent, la collecte et le traitement d'identifiants SSID sont des procédés disproportionnés lorsqu'il s'agit d'offrir des services de géolocalisation basés sur le mappage de la position de points d'accès Wi-Fi.

5.4 Informations

Les différents responsables du traitement doivent s'assurer que les propriétaires de dispositifs mobiles intelligents sont dûment informés des éléments clés du traitement, conformément à l'article 10 de la directive sur la protection des données, tels que leur identité en tant que responsables du traitement, les finalités du traitement, le type de données, la durée du traitement, les droits des personnes concernées d'accéder à leurs données, de les rectifier ou de les supprimer et leur droit de retirer leur consentement.

La validité du consentement est inextricablement liée à la qualité des informations concernant le service. Les informations doivent être claires, exhaustives, compréhensibles pour un large public non initié, et accessibles facilement et en permanence.

---

[15] Exemple d'utilisation possible:

1. Une personne concernée se rend sur une page Web spécifique, sur laquelle elle peut entrer l'adresse MAC de son point d'accès Wi-Fi.
2. Si l'adresse MAC apparaît dans la base de données avec les points d'accès Wi-Fi mappés, le responsable du traitement peut faire apparaître une page de vérification contenant un script qui demande la table ARP du dispositif internet. En théorie, il est possible de voir les adresses MAC de réseau WLAN par l'intermédiaire de la commande «ARP –a». À l'aide du code contenu dans le navigateur, tel que Java, cette table ARP peut être produite en arrière-plan.
3. Si l'adresse MAC n'apparaît pas dans la table ARP, il est déterminé que l'utilisateur connecté au réseau local sans fil est également celui ayant accès à l'adresse MAC de réseau WLAN locale. Le responsable du traitement vérifie ainsi automatiquement et facilement la demande de suppression.

Les informations doivent toucher un public très large. Les responsables du traitement ne peuvent supposer que leurs clients sont des personnes techniquement compétentes, simplement parce qu'elles possèdent un dispositif mobile intelligent. Les informations doivent être adaptées à l'âge si le responsable du traitement sait qu'il s'adresse à un public jeune.

Si des fournisseurs d'applications de géolocalisation comptent calculer les positions d'un dispositif plus d'une fois, ils doivent tenir leurs clients informés aussi longtemps qu'ils traitent des données de localisation. Ils doivent également permettre à leurs clients de prolonger ou de révoquer leur consentement. Afin d'atteindre ces objectifs, les fournisseurs d'applications devraient travailler en étroite collaboration avec le développeur du système d'exploitation. Sur le plan technique, le développeur est le mieux placé pour créer un rappel visible en permanence indiquant que des données de localisation sont en cours de traitement. Le développeur est également le mieux placé pour faire en sorte qu'aucune des applications proposées ne surveille en secret l'emplacement des dispositifs mobiles intelligents.

Si le développeur du système d'exploitation a créé une fonctionnalité «phone home» ou un autre moyen pour obtenir l'accès à des données stockées sur le dispositif, ou qu'il obtient l'accès à des données de localisation par d'autres moyens, par l'intermédiaire d'annonceurs tiers par exemple, il doit informer la personne concernée au préalable des raisons (spécifiques et légitimes) pour lesquelles il traite ces données et de la durée du traitement.

L'obligation de tenir informées les personnes concernées s'applique également aux responsables de bases de données comportant des points d'accès Wi-Fi géolocalisés. Ils doivent informer le grand public de manière adéquate sur leur identité et les finalités du traitement ainsi que sur d'autres données pertinentes. La simple mention d'une éventuelle collecte de données concernant des points d'accès Wi-Fi dans une déclaration de confidentialité spécifique à l'intention des utilisateurs d'une application de géolocalisation n'est pas suffisante. Il existe suffisamment de moyens, en ligne et hors ligne, permettant d'informer le grand public.

5.5 Droits des personnes concernées

Les personnes concernées sont en droit d'obtenir, de la part des différents responsables du traitement, un accès aux données de localisation obtenues à partir de leurs dispositifs mobiles intelligents, ainsi que des informations sur les finalités du traitement et les destinataires ou catégories de destinataires à qui les données ont été divulguées. Les informations doivent être fournies dans une version directement lisible, à savoir, sous la forme de positions géographiques, et non pas de numéros abstraits de stations de base, par exemple.

Les personnes concernées sont également en droit d'accéder aux profils possibles basés sur ces données de localisation. Si les informations de localisation sont stockées, les utilisateurs devraient être autorisés à mettre à jour, rectifier ou effacer ces informations.

Le groupe de travail recommande aux responsables du traitement de chercher des moyens sécurisés permettant de fournir un accès direct en ligne aux données de localisation et aux profils possibles. Il est essentiel qu'un tel accès soit fourni sans demander de données à caractère personnel supplémentaires pour vérifier l'identité des personnes concernées.

5.6 Délais de conservation

Les fournisseurs de services de géolocalisation et d'application devraient déterminer un délai de conservation pour les données de localisation dont la durée n'excède pas celle nécessaire aux fins pour lesquelles les données ont été collectées ou font l'objet d'un traitement ultérieur. Ils doivent s'assurer que les données de géolocalisation, ou les profils fondés sur ces données, sont effacées après une période de temps justifiée.

Dans le cas où il a été prouvé qu'il est nécessaire pour le développeur du système d'exploitation et/ou le responsable d'une infrastructure de géolocalisation de recueillir des données d'historique de localisation anonymes dans le but de mettre à jour ou d'améliorer leur service, il convient de faire preuve d'une extrême prudence pour éviter de rendre ces données identifiables (indirectement). En particulier, même si le dispositif mobile est identifié à l'aide d'un identifiant unique (UDID) attribué de manière aléatoire, un tel numéro unique ne devrait être stocké que pour une période maximale de 24 heures à des fins opérationnelles. Après cette période, l'identifiant UDID devrait être anonymisé davantage en tenant compte du fait qu'une véritable anonymisation est de plus en plus difficile à obtenir et que la combinaison des données de localisation peut tout de même aboutir à une identification. Un tel UDID ne devrait ni pouvoir être associé à de précédents ou futurs UDID attribués au dispositif, ni être associé à un quelconque identifiant fixe de l'utilisateur ou du téléphone (tel qu'une adresse MAC, un numéro IMEI ou IMSI, ou tout autre numéro de compte).

En ce qui concerne des données relatives à des points d'accès Wi-Fi, une fois que l'adresse MAC d'un point d'accès Wi-Fi est associée à une nouvelle position, sur la base des observations continues de propriétaires de dispositifs mobiles intelligents, la position précédente doit être immédiatement supprimée, pour éviter toute utilisation ultérieure des données à des fins inappropriées, telles que des démarches commerciales visant des personnes ayant modifié leur position.

6. Conclusions

Les technologies de géolocalisation qui utilisent les données de stations de base, les données GPS et les points d'accès Wi-Fi mappés, permettent à toutes sortes de responsables du traitement de localiser des dispositifs mobiles intelligents pour des finalités allant de la publicité comportementale à la surveillance des enfants.

Étant donné que les téléphones intelligents et les tablettes électroniques sont inextricablement liés à leur propriétaire, les schémas de déplacement des dispositifs donnent une vision détaillée de l'intimité de la vie privée des propriétaires. L'un des principaux risques est que les propriétaires ignorent qu'ils transmettent leur position et à qui ils les transmettent. Un autre risque est que l'autorisation donnée à certaines applications d'utiliser les données de localisation n'est pas valable, car les informations concernant les éléments clés du traitement sont incompréhensibles, désuètes ou inadéquates.

Les obligations diffèrent en fonction des parties intéressées, qui vont des développeurs des systèmes d'exploitation aux fournisseurs d'application et parties telles que les sites de socialisation qui intègrent dans leurs plates-formes des fonctions de localisation destinées à des dispositifs mobiles.

6.1 Cadre juridique

- Le cadre juridique de l'UE pour l'utilisation de données de géolocalisation provenant de dispositifs mobiles intelligents est fourni principalement par la directive sur la protection des données. Les données de localisation provenant de dispositifs mobiles intelligents sont des données à caractère personnel. La combinaison de l'adresse MAC unique et de la position calculée d'un point d'accès Wi-Fi devrait être traitée de la même manière que des données à caractère personnel.
- De plus, la directive 2002/58/CE révisée sur la vie privée et les communications électroniques ne s'applique qu'au traitement de données de stations de base par des opérateurs de télécommunications.

6.2 Responsables du traitement

- Il est possible de distinguer trois types de responsables du traitement: les responsables d'infrastructure de géolocalisation (notamment les responsables de points d'accès Wi-Fi mappés); les fournisseurs d'applications et de services de géolocalisation; et les développeurs de système d'exploitation de dispositifs mobiles intelligents.

6.3 Motif légitime

- Étant donné que les données de dispositifs mobiles intelligents révèlent des détails intimes sur la vie privée de leur propriétaire, le principal motif légitime applicable est le consentement préalable en connaissance de cause.
- Le consentement ne peut pas être obtenu par l'intermédiaire de l'acceptation des conditions générales.
- Le consentement doit être spécifique pour chacune des différentes finalités pour lesquelles les données sont traitées, par exemple l'établissement de profils et/ou le ciblage comportemental par le responsable du traitement. Si les finalités du traitement changent de manière significative, le responsable du traitement doit chercher à obtenir une nouvelle fois le consentement spécifique.
- Par défaut, les services de localisation doivent être désactivés. Le fait de proposer la possibilité de renoncer au transfert de données ne constitue pas un mécanisme adéquat pour obtenir le consentement en connaissance de cause d'un utilisateur.
- Le consentement pose problème en ce qui concerne les travailleurs et les enfants. En ce qui concerne les travailleurs, les employeurs ne peuvent utiliser cette technologie que lorsqu'il est possible de prouver qu'elle est nécessaire pour une finalité légitime, et que les mêmes objectifs ne peuvent pas être atteints à l'aide de moyens moins intrusifs. En ce qui concerne les enfants, c'est à leurs parents de juger si l'utilisation d'une telle application est justifiée dans certaines circonstances. Les parents doivent à tout le moins informer leurs enfants, et dès que raisonnablement possible, permettre à leurs enfants de participer à la décision d'utiliser une telle application.
- Le groupe de travail recommande de limiter la portée du consentement dans le temps et de recontacter les utilisateurs au moins une fois par an. Il recommande également de détailler suffisamment le consentement en ce qui concerne la précision des données de localisation.
- Les personnes concernées doivent pouvoir retirer facilement leur consentement, sans aucune conséquence négative pour l'utilisation de leur dispositif.
- En ce qui concerne le mappage de points d'accès Wi-Fi, les sociétés peuvent avoir un intérêt légitime à recueillir et à traiter les adresses MAC et les positions calculées de points d'accès Wi-Fi dans le but spécifique d'offrir des services de géolocalisation. La mise en balance des droits du responsable du traitement, d'une part, et des droits des personnes concernées, d'autre part, nécessite que le responsable du traitement accorde

aux utilisateurs le droit de renoncer de manière aisée et définitive à participer à la base de données, sans exiger la fourniture de données à caractère personnel supplémentaires.

6.4 Les informations

- Les informations doivent être claires, exhaustives, compréhensibles pour un large public non initié et accessibles facilement et en permanence.
- La validité du consentement est inextricablement liée à la qualité des informations concernant le service.
- Les tiers, tels que les navigateurs et les sites de socialisation ont un rôle essentiel à jouer lorsqu'il s'agit de la visibilité et de la qualité des informations concernant le traitement des données de géolocalisation.

6.5 Droits des personnes concernées

- Les différents responsables du traitement d'informations de géolocalisation provenant de dispositifs mobiles doivent permettre à leurs clients d'accéder à leurs données de localisation dans une version directement lisible et les autoriser à les rectifier ou à les supprimer sans recueillir une quantité excessive de données à caractère personnel.
- Les personnes concernées ont également le droit d'accéder aux éventuels profils, de les rectifier et de les supprimer en fonction de ces données de localisation.
- Le groupe de travail recommande la création d'un accès en ligne (sécurisé).

6.6 Délais de conservation

- Les fournisseurs d'applications ou de services de géolocalisation doivent mettre en œuvre des politiques de conservation garantissant que des données de géolocalisation ou des profils découlant de telles données sont supprimés après une période de temps justifiée.
- Si le développeur du système d'exploitation et/ou le responsable du traitement de l'infrastructure de géolocalisation traitent un numéro unique tel qu'une adresse MAC ou un identifiant UDID en rapport avec des données de localisation, le numéro d'identification unique ne peut être stocké que pour une période maximale de 24 heures, à des fins opérationnelles.

Fait à Bruxelles,
le 16 mai 2011

Pour le groupe de travail
Le président
Jacob KOHNSTAMM