GROUPE DE TRAVAIL «ARTICLE 29» SUR LA PROTECTION DES DONNÉES

00461/13/FR
GT 202

Avis 02/2013 sur les applications destinées aux dispositifs intelligents

Adopté le 27 février 2013

Le groupe de travail a été institué en vertu de l'article 29 de la directive 95/46/CE. Il s'agit d'un organe consultatif européen indépendant sur la protection des données et de la vie privée. Ses missions sont définies à l'article 30 de la directive 95/46/CE et à l'article 15 de la directive 2002/58/CE.

Le secrétariat est assuré par la direction C (Droits fondamentaux et citoyenneté de l'Union) de la direction générale de la justice de la Commission européenne, B-1049 Bruxelles, Belgique, bureau n° MO59-02/013.
Site web: http://ec.europa.eu/justice/data-protection/index_en.htm

Résumé

Des centaines de milliers d'applications différentes sont proposées par divers magasins d'applications pour chaque type de dispositif intelligent courant. Il a été constaté que plus de 1 600 nouvelles applications sont ajoutées chaque jour dans ces magasins et qu'un utilisateur moyen télécharge 37 applications. Les applications peuvent être proposées à l'utilisateur final gratuitement ou pour un coût initial modique. Quant au nombre d'utilisateurs, il peut varier de quelques personnes seulement à plusieurs millions.

Les applications sont en mesure de collecter de grandes quantités de données en provenance des dispositifs (qu'il s'agisse des données stockées dans l'appareil par l'utilisateur ou des données fournies par les différents capteurs, comme les données de localisation par exemple) et de les traiter afin de fournir à l'utilisateur final des services nouveaux et innovants. Cependant, ces mêmes sources de données peuvent faire l'objet d'un traitement ultérieur, le plus souvent en vue de générer des revenus, à l'insu de l'utilisateur final ou d'une manière non souhaitée par ce dernier.

Les développeurs d'applications ignorant l'existence d'obligations en matière de protection des données peuvent être à l'origine de risques importants pour la vie privée et la réputation de l'utilisateur de dispositifs intelligents. En matière de protection des données, les principaux risques pour l'utilisateur final sont l'absence de transparence et de connaissance préalable des types de traitement qu'une application est susceptible d'effectuer, ainsi que l'absence de consentement explicite de la part de l'utilisateur final avant le début du traitement des données. La médiocrité des mesures de sécurité, une tendance manifeste en faveur de la maximisation des données ainsi que la diversité des finalités pour lesquelles les données à caractère personnel sont recueillies renforcent encore les risques en matière de protection des données rencontrés dans l'environnement applicatif actuel.

En matière de protection des données, d'autres risques élevés découlent du degré de fragmentation de l'environnement dans lequel évoluent les nombreuses parties participant au développement des applications. Ces différents intervenants sont les développeurs, les propriétaires et les magasins d'applications, les fabricants de systèmes d'exploitation et de dispositifs, ainsi que d'autres tiers éventuellement concernés par la collecte et le traitement de données à caractère personnel en provenance des dispositifs intelligents, tels que les fournisseurs de solutions analytiques et les annonceurs. La plupart des conclusions et des recommandations du présent avis s'adressent aux développeurs d'applications (dans la mesure où ceux-ci contrôlent en grande partie la manière précise dont le traitement est effectué ou dont les informations sont présentées au sein de l'application). Bien souvent, cependant, afin de respecter les normes les plus strictes en matière de protection de la vie privée et des données, les développeurs d'applications doivent collaborer dans cet écosystème avec d'autres parties. Cette collaboration est particulièrement importante au niveau de la sécurité, dans la mesure où la longue chaîne d'intervenants est aussi forte que le plus faible de ses maillons.

Parmi les nombreux types de données disponibles sur les dispositifs mobiles intelligents, beaucoup sont des données à caractère personnel. Le cadre juridique pertinent à cet égard est la directive sur la protection des données, ainsi que la directive «vie privée et communications électroniques», dans sa partie relative à la protection des appareils mobiles relevant de la vie privée des utilisateurs. Ces règles concernent toutes les applications destinées aux utilisateurs

au sein de l'Union européenne, indépendamment de l'endroit où se situent le développeur ou le magasin d'applications.

Le présent avis du groupe de travail vise à clarifier le cadre juridique régissant le traitement des données à caractère personnel dans le développement, la distribution et l'utilisation d'applications destinées aux dispositifs intelligents, en mettant en exergue l'obligation de consentement, les principes de limitation de la finalité et de minimisation des données, la nécessité de prendre les mesures de sécurité adéquates, l'obligation d'informer correctement l'utilisateur final, les droits de ce dernier, les durées de conservation raisonnables et, plus particulièrement, le traitement loyal des données collectées en provenance et au sujet des enfants.

Table des matières

1. Introduction

On entend par «applications» des applications logicielles généralement conçues pour effectuer une tâche spécifique et destinées à un groupe particulier de dispositifs intelligents tels que les téléphones intelligents, les tablettes et les télévisions connectées à l'Internet. Elles organisent les informations d'une manière adaptée aux caractéristiques spécifiques du dispositif et interagissent en général étroitement avec les éléments matériels et les fonctionnalités du système d'exploitation des dispositifs.

Des centaines de milliers d'applications différentes sont proposées par divers magasins d'applications pour chaque type de dispositif intelligent courant. Les finalités auxquelles les applications répondent sont variées et comprennent entre autres la navigation sur Internet, la communication (courriels, téléphonie et messagerie Internet), le divertissement (jeux, films/vidéos et musique), le réseautage social, les applications bancaires et les services de localisation. Il a été constaté que plus de 1 600 nouvelles applications sont ajoutées chaque jour dans les magasins d'applications[1] et qu'un utilisateur de téléphone intelligent moyen télécharge 37 applications[2]. Les applications peuvent être proposées à l'utilisateur final gratuitement ou pour un coût initial modique. Quant au nombre d'utilisateurs, il peut varier de quelques personnes seulement à plusieurs millions.

Le système d'exploitation sous-jacent inclura également des structures de données ou des logiciels importants pour les services de base du dispositif intelligent, comme le carnet d'adresses d'un téléphone intelligent, par exemple. Le système d'exploitation est conçu de manière à permettre aux applications d'accéder à ces éléments à l'aide d'interfaces de programmes d'application (API). Ces API autorisent l'accès à une multitude de capteurs qui peuvent être présents dans les dispositifs intelligents. Ces capteurs comprennent: un gyroscope, une boussole numérique et un accéléromètre pour la vitesse et la direction de mouvement; des caméras avant et arrière pour l'enregistrement de vidéos et la prise de photos; et un microphone pour les enregistrements audio. Les dispositifs intelligents peuvent être également munis de capteurs de proximité[3] et se connecter via une multitude d'interfaces de réseaux de type Wi-Fi, Bluetooth, NFC ou encore Ethernet. Enfin, une position précise peut être déterminée à l'aide de services de géolocalisation (tels que décrits dans l'avis 13/2011 du groupe de travail «Article 29» sur les services de géolocalisation des dispositifs mobiles intelligents[4]). Le type, la précision et la fréquence des données du capteur varient en fonction du dispositif et du système d'exploitation.

---

[1] Rapport de «ConceivablyTech» du 19 août 2012, disponible à l'adresse électronique www.conceivablytech.com/10283/business/apple-app-store-to-reach-1mapps-this-year-sort-of. Cité par Kamala D. Harris, procureur général du département de la justice de l'État de Californie, «Privacy on the go, Recommendations for the mobile ecosystem», janvier 2013, http://oag.ca.gov/sites/all/files/pdfs/privacy/privacy_on_the_go.pdf

[2] Il s'agit d'une estimation à l'échelle mondiale pour 2012 réalisée par ABI Research, http://www.abiresearch.com/press/smartphone-utilisateurs-worldwide-will-download-37-apps-o

[3] Un capteur en mesure de détecter la présence d'un objet physique sans contact physique. Voir: http://www.w3.org/TR/2012/WD-proximity-20121206/

[4] Voir l'avis 13/2011 du groupe de travail «Article 29» sur les services de géolocalisation des dispositifs mobiles intelligents (mai 2011), http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp185_fr.pdf.

Grâce aux API, les développeurs d'applications peuvent collecter des données en continu, accéder aux données de contact ou en écrire, envoyer des courriels, des messages courts (SMS) ou des messages sur les réseaux sociaux, lire/modifier/supprimer le contenu de cartes SD, enregistrer des messages audio, utiliser la caméra et accéder aux photos stockées, consulter l'état et l'identité du téléphone, modifier les paramètres généraux du système et empêcher la mise en veille du téléphone. Les API peuvent également fournir des informations concernant le dispositif lui-même à l'aide d'un ou plusieurs identifiant(s) unique(s) ainsi que des renseignements sur les autres applications présentes. Ces sources de données peuvent faire l'objet d'un traitement ultérieur, le plus souvent en vue de générer des revenus, à l'insu de l'utilisateur final ou d'une manière non souhaitée par ce dernier.

Le présent avis vise à clarifier le cadre juridique régissant le traitement des données à caractère personnel dans la distribution et l'utilisation d'applications destinées aux dispositifs intelligents. Il couvre également la question des traitements de données susceptibles d'être effectués ultérieurement en dehors de l'application, tels que l'utilisation des données collectées pour la création de profils ou le ciblage des utilisateurs. Cet avis propose une analyse des principaux risques en matière de protection des données, fournit une description des différentes parties prenantes et met en évidence les diverses responsabilités sur le plan juridique. Les parties concernées sont: les développeurs, les propriétaires et les magasins d'applications, les fabricants de systèmes d'exploitation et de dispositifs, ainsi que d'autres tiers participant éventuellement à la collecte et au traitement de données à caractère personnel en provenance de dispositifs intelligents, tels que les fournisseurs de solutions analytiques et les annonceurs.

Le présent avis met en exergue l'obligation de consentement, les principes de limitation de la finalité et de minimisation des données, la nécessité de prendre les mesures de sécurité adéquates, l'obligation d'informer correctement l'utilisateur final, les droits de ce dernier, les durées de conservation raisonnables et, plus particulièrement, le traitement loyal des données collectées en provenance et au sujet des enfants.

Bien que son champ d'application englobe de nombreux types de dispositifs intelligents différents, le présent document vise en particulier les applications destinées aux dispositifs mobiles intelligents.

2. Les risques en matière de protection des données

L'étroite interaction avec le système d'exploitation permet aux applications d'accéder à bien plus de données qu'un navigateur Internet traditionnel[5]. Les applications sont en mesure de collecter de grandes quantités de données à partir des dispositifs (données de localisation, données stockées dans l'appareil par l'utilisateur ou données provenant des différents capteurs) et de les traiter afin de fournir à l'utilisateur final des services nouveaux et innovants.

En matière de protection des données, il existe un risque élevé découlant du niveau de fragmentation de l'environnement dans lequel évoluent les nombreuses parties participant au développement des applications. Une donnée peut être transmise en temps réel par le

[5] Aujourd'hui, cependant, sous l'impulsion des concepteurs de jeux Internet, les navigateurs Internet bénéficient d'un accès plus large aux données provenant des capteurs installés dans les dispositifs des utilisateurs finaux.

dispositif pour être traitée à travers le monde ou être copiée entre les différentes chaînes de tiers. Certaines des applications les plus connues sont élaborées par de grandes sociétés technologiques mais bien d'autres sont conçues par de petites start-ups. Un programmeur seul, avec une idée, et peu ou pas de compétences de programmation préalables, peut atteindre un large public en très peu de temps. Les développeurs d'applications ignorant l'existence d'obligations en matière de protection des données peuvent être à l'origine de risques importants pour la vie privée et la réputation de l'utilisateur de dispositifs intelligents. Dans le même temps, des services de tiers tels que les annonces publicitaires, connaissent un développement rapide et peuvent, s'ils sont intégrés de manière inconsidérée par un développeur d'applications, donner accès à d'importantes quantités de données à caractère personnel.

En matière de protection des données, les principaux risques pour l'utilisateur final sont l'absence de transparence et de connaissance préalable des types de traitement qu'une application est susceptible d'effectuer, ainsi que l'absence de consentement explicite de la part de l'utilisateur final avant le début du traitement. L'insufisance des mesures de sécurité, une tendance manifeste en faveur de la maximisation des données ainsi que la diversité des finalités justifiant la collecte des données à caractère personnel renforcent encore les risques en matière de protection des données rencontrés dans l'environnement applicatif actuel. Bon nombre de ces risques ont déjà été analysés et couverts par d'autres régulateurs internationaux, tels que la Commission fédérale du commerce (FTC) aux États-Unis, le Commissariat à la protection de la vie privée au Canada, et le procureur général du département de la justice de l'État de Californie[6].

- Un des principaux risques en matière de protection des données est l'absence de transparence. Les options proposées par les fabricants de systèmes d'exploitation et les magasins d'applications obligent les développeurs d'applications à mettre les informations complètes à la disposition de l'utilisateur final en temps opportun. Toutefois, tous les développeurs d'applications ne le font pas dans la mesure où de nombreuses applications n'ont pas de politique de protection de la vie privée ou n'informent pas clairement les utilisateurs potentiels du type de données à caractère personnel susceptibles d'être traitées par l'application, ni de la finalité du traitement. Cette absence de transparence ne se limite pas uniquement aux applications gratuites ou conçues par des développeurs inexpérimentés, comme le démontre une étude récente selon laquelle seules 61,3 % des 150 applications les plus courantes ont une politique de protection de la vie privée[7].

---

[6] Voir, entre autres, le rapport du personnel de la FTC «Mobile Privacy Disclosures, Building Trust Through Transparency», février 2013, http://www.ftc.gov/os/2013/02/130201mobileprivacyreport.pdf; le rapport du personnel de la FTC «Mobile Apps for Kids: Current Privacy Disclosures are Disappointing», février 2012, http://www.ftc.gov/os/2012/02/120216mobile_apps_kids.pdf; ainsi que le rapport de suivi, «Mobile Apps for Kids: Disclosures Still Not Making the Grade», décembre 2012, http://www.ftc.gov/os/2012/12/121210mobilekidsappreport.pdf.
Le rapport du Commissariat à la protection de la vie privée du Canada, «Une occasion à saisir : développer des applis mobiles dans le respect du droit à la vie privée», octobre 2012, http://www.priv.gc.ca/information/pub/gd_app_201210_e.pdf, Kamala D. Harris, procureur général du département de la justice de l'État de Californie, «Privacy on the go, Recommendations for the mobile ecosystem», janvier 2013, http://oag.ca.gov/sites/all/files/pdfs/privacy/privacy_on_the_go.pdf

[7] Étude du forum «Future of Privacy» (FPF) sur les applications mobiles, juin 2012, http://www.futureofprivacy.org/wp-content/uploads/Mobile-Apps-Study-June-2012.pdf

- Le manque de transparence est étroitement lié à l'absence de consentement libre et informé. Une fois que l'application est téléchargée, le consentement de l'utilisateur final se limite souvent à une case à cocher précisant qu'il accepte les termes et conditions, sans que soit même proposée une option «Non, merci». Selon une étude de GSMA de septembre 2011, 92 % des utilisateurs d'applications souhaitent pouvoir bénéficier d'un choix plus détaillé[8].

- L'insuffisance des mesures de sécurité peut donner lieu à un traitement non autorisé des données à caractère personnel (sensibles), par exemple en cas de violation de ces données chez le développeur d'applications ou de fuite dans l'application même.

- Un autre risque en matière de protection des données est lié au non respect (intentionnel ou par ignorance) du principe de limitation de la finalité en vertu duquel les données à caractère personnel ne peuvent être collectées et traitées qu'à des fins spécifiques et légitimes. Il se peut que les données à caractère personnel collectées par des applications soient transmises à grande échelle à certains tiers, à des fins variées ou floues telles que des «études de marché». Le même mépris alarmant est affiché à l'égard du principe de minimisation des données. Des recherches récentes ont révélé que de nombreuses applications collectent de gros volumes de données en provenance des téléphones intelligents, sans qu'il y ait le moindre rapport significatif avec la fonctionnalité apparente de l'application[9].

3 Les principes applicables en matière de protection des données

3.1 La législation en vigueur

Le cadre juridique de référence de l'Union européenne est la directive 95/46/CE relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel. Celle-ci est applicable chaque fois que l'utilisation d'applications présentes dans les dispositifs intelligents implique le traitement de données à caractère personnel relatives à des personnes. Afin de déterminer la législation applicable, il est impératif de définir dans un premier temps le rôle des différentes parties concernées: l'identification du ou des responsable(s) du traitement effectué à l'aide des applications mobiles est particulièrement cruciale pour le choix de la législation applicable. Le lieu d'établissement du responsable du traitement est un élément décisif pour l'application de la législation de l'Union européenne sur la protection des données, bien que ce ne soit pas le seul critère. Conformément à l'article 4, paragraphe 1, point a), de la directive sur la protection des données, les dispositions nationales d'un État membre sont applicables aux traitements de données à caractère personnel lorsque le traitement est effectué «dans le cadre des activités d'un établissement» du responsable du traitement sur le territoire de l'État membre. En application de l'article 4, paragraphe 1, point c), de la directive sur la protection des données, les dispositions nationales d'un État membre sont également applicables lorsque le responsable du traitement *n'est pas établi* sur le territoire de la Communauté et recourt à des moyens situés sur le territoire dudit

---

[8] «*89% [des utilisateurs] estiment qu'il est important de savoir à quel moment leurs informations personnelles sont partagées par une application et de pouvoir conserver ou abandonner cette application.*» Source: «User perspectives on mobile privacy», septembre 2011, http://www.gsma.com/publicpolicy/wp-content/uploads/2012/03/futuresightuserperspectivesonuserprivacy.pdf

[9] Wall Street Journal, «Your Apps Are Watching You», http://online.wsj.com/article/SB10001424052748704694004576020083703574602.html

État membre. Étant donné que le dispositif est un moyen permettant le traitement de données à caractère personnel en provenance et au sujet de l'utilisateur, ce critère est généralement respecté[10].Toutefois, ce dernier point n'est pertinent que lorsque le responsable du traitement n'est pas établi dans l'Union européenne.

En conséquence, dès lors qu'une partie participant au développement, à la distribution et à l'exploitation d'applications est considérée comme étant le responsable du traitement, celle-ci est responsable, seule ou conjointement avec d'autres parties, du respect de toutes les obligations prévues par la directive sur la protection des données. La détermination du rôle des parties participant aux activités associées aux applications mobiles fera l'objet d'une analyse plus détaillée au point 3.3 ci-dessous.

Outre la directive sur la protection des données, la directive «vie privée et communications électroniques» (2002/58/CE, telle que modifiée par la directive 2009/136/CE), fixe une norme spécifique pour toutes les parties, quel que soit leur lieu d'établissement dans le monde, souhaitant stocker des informations, ou accéder à des informations déjà stockées, dans les dispositifs d'utilisateurs situés dans l'Espace économique européen (EEE).

L'article 5, paragraphe 3, de la directive «vie privée et communications électroniques» dispose que *le stockage d'informations, ou l'obtention de l'accès à des informations déjà stockées, dans l'équipement terminal d'un abonné ou d'un utilisateur n'est permis qu'à condition que l'abonné ou l'utilisateur ait donné son accord, après avoir reçu, dans le respect de la directive 95/46/CE, une information claire et complète, entre autres sur les finalités du traitement. (...)*

Alors que de nombreuses dispositions de la directive «vie privée et communications électroniques» ne s'appliquent qu'aux fournisseurs de services de communications électroniques accessibles au public et aux fournisseurs de réseaux publics de communication dans la Communauté, l'article 5, paragraphe 3, s'applique à toute entité souhaitant stocker des informations sur des dispositifs intelligents ou lire des informations provenant de ces dispositifs. Cet article s'applique indépendamment de la nature de l'entité (qu'il s'agisse d'une entité publique ou privée, d'un programmeur privé ou d'une grande entreprise, d'un responsable du traitement, d'un sous-traitant ou d'un tiers).

L'obligation de consentement visée à l'article 5, paragraphe 3, s'applique à <u>toute information</u>, quelle que soit la nature des données que l'on stocke ou auxquelles on accède. Le champ d'application ne se limite pas aux données à caractère personnel; il couvre tous les types de données stockées dans le dispositif.

L'obligation de consentement visée à l'article 5, paragraphe 3, de la directive «vie privée et communications électroniques» s'applique aux services proposés «*dans la Communauté*», c'est-à-dire à toutes les personnes vivant dans l'Espace économique européen, quelle que soit la localisation du fournisseur de services. Il est important que les développeurs d'applications soient conscients du fait que les deux directives sont juridiquement contraignantes dans la mesure où les droits des individus sont inaliénables et non soumis à des restrictions contractuelles. Cela signifie que l'applicabilité de la législation européenne sur la protection

[10] Dans la mesure où l'application génère un trafic de données à caractère personnel vers les responsables du traitement. Ce critère pourrait ne pas être respecté si les données étaient traitées exclusivement localement, dans le dispositif même.

de la vie privée ne peut être rejetée sur la base d'une déclaration unilatérale ou en vertu d'un accord contractuel[11].

3.2 Le traitement des données à caractère personnel par les applications

De nombreux types de données stockées sur un dispositif intelligent ou générées par ce dernier sont des données à caractère personnel. Selon le considérant n° 24 de la directive «vie privée et communications électroniques»:

> *«L'équipement terminal de l'utilisateur d'un réseau de communications électroniques ainsi que toute information stockée sur cet équipement relèvent de la vie privée de l'utilisateur, qui doit être protégée au titre de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales.»*

Les données sont à caractère personnel dès lors qu'elles se rapportent à une personne directement (par son nom, par exemple) ou indirectement identifiable auprès du responsable du traitement ou d'un tiers. Elles peuvent concerner le propriétaire du dispositif ou toute autre personne, comme les amis dont les coordonnées figurent dans un carnet d'adresses[12]. Les données peuvent être collectées et traitées dans le dispositif même ou ailleurs après transfert, sur les infrastructures de développeurs d'applications ou de tiers par exemple, à l'aide d'une connexion vers une API externe, en temps réel et à l'insu de l'utilisateur final.

Les données à caractère personnel dont l'incidence sur la vie privée de l'utilisateur et d'autres personnes peut être significative sont, entre autres:

- la localisation;
- les contacts;
- les identifiants uniques des dispositifs et des clients (tels que l'IMEI[13], l'IMSI[14], l'UDID[15] et le numéro du téléphone mobile);
- l'identité de la personne concernée;
- l'identité du téléphone (c.-à-d. le nom du téléphone[16]);
- les données relatives aux cartes de crédit et aux paiements;
- les journaux d'appels, les SMS ou la messagerie instantanée;
- l'historique de navigation;
- les courriels;
- les données d'authentification pour les services de la société de l'information (notamment les services à caractère social);
- les photos et les vidéos;
- les éléments de biométrie (par exemple, des images de référence pour la reconnaissance faciale ou des modèles d'empreintes digitales).

---

[11] Par exemple, des clauses selon lesquelles la seule juridiction compétente serait établie en dehors de l'EEE.

[12] Les données peuvent être (i) générées automatiquement par le dispositif, sur la base de fonctionnalités prédéterminées par le fabricant du système d'exploitation et/ou du dispositif ou par l'opérateur de téléphonie mobile concerné (par exemple, les données de géolocalisation, les paramètres du réseau, l'adresse IP); (ii) générées par l'utilisateur à l'aide d'applications (listes de contacts; notes, photos); (iii) générées par les applications (par exemple, l'historique de navigation).

[13] Identité internationale de l'équipement mobile.

[14] Identité internationale de l'abonné mobile.

[15] Identificateur unique du dispositif.

[16] Les utilisateurs ont tendance à donner leur nom véritable à leur téléphone: «iPhone de John Doe».

3.3 Les parties associées au traitement des données

De nombreuses parties différentes participent au développement, à la distribution et à l'exploitation d'applications, et chacune d'entre elles peut assumer différentes responsabilités en matière de protection des données.

Les parties concernées peuvent être classées en quatre grandes catégories: (i) les développeurs d'applications (y compris les propriétaires d'applications)[17]; (ii) les fabricants de systèmes d'exploitation et de dispositifs[18]; (iii) les magasins d'applications (les distributeurs de l'application) et, enfin, (iv) les autres parties associées au traitement de données à caractère personnel. Dans certains cas, les responsabilités en matière de protection des données sont partagées, en particulier lorsque la même entité est impliquée à différents niveaux, par exemple lorsque le fabricant du système d'exploitation contrôle également le magasin d'applications.

L'utilisateur final doit également assumer une juste responsabilité dans la mesure où il crée et stocke des données à caractère personnel avec son dispositif mobile. Si les données sont traitées à des fins personnelles ou domestiques, l'article 3, paragraphe 2, de la directive sur la protection des données n'est pas applicable et l'utilisateur est dispensé des obligations formelles liées à la protection des données. Si, toutefois, l'utilisateur décide de partager les données à l'aide d'une application, par exemple en rendant les informations publiques auprès d'un nombre indéterminé de personnes[19] au moyen d'une application de réseau social, le traitement des informations n'est plus couvert par l'exemption domestique[20].

3.3.1 Les développeurs d'applications

Les développeurs d'applications créent des applications et/ou les mettent à la disposition de l'utilisateur final. Cette catégorie comprend des organisations du secteur public et privé qui externalisent le développement des applications ainsi que les sociétés et les personnes qui créent et distribuent les applications. Elles conçoivent et/ou créent le logiciel qui sera installé sur les téléphones intelligents et décident donc dans quelle mesure les applications accéderont aux différentes catégories de données à caractère personnel en vue de leur traitement dans le dispositif et/ou à l'aide de ressources de télétraitement (unités de traitement des développeurs d'application ou de tiers).

Dans la mesure où le développeur d'applications fixe les finalités et les moyens du traitement des données à caractère personnel dans les dispositifs intelligents, il devient le responsable du traitement conformément à l'article 2, point d), de la directive sur la protection des données. Dans ce cas, il est tenu de respecter les dispositions de l'ensemble de la directive sur la

---

[17] Bien que le groupe de travail utilise la terminologie courante «développeur d'applications», il souligne le fait que ces termes ne se limitent pas aux programmeurs ou aux concepteurs techniques d'applications mais recouvrent également les propriétaires d'applications, à savoir les sociétés ou organisations qui commandent le développement d'applications et décident de leur finalité.

[18] Dans certains cas, le fabricant du système d'exploitation est également le fabricant du dispositif tandis que dans d'autres cas, le fabricant du dispositif est une société différente du fournisseur du système d'exploitation.

[19] Voir les affaires de la Cour européenne de justice: l'affaire C-101/01, procédure pénale contre Bodil Lindqvist, arrêt du 6 novembre 2003, et l'affaire C-73/07, Tietosuojavaltuutettu contre Satakunnan Markkinapörssi Oy et Satamedia Oy, arrêt du 16 décembre 2008.

[20] Voir l'avis 5/2009 du groupe de travail «Article 29» sur les réseaux sociaux en ligne (juin 2009), http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp163_fr.pdf

protection des données. Les dispositions principales sont décrites aux points 3.4 à 3.10 du présent avis.

Même lorsque l'exemption domestique s'applique à un utilisateur, le développeur d'applications conserve son statut de responsable du traitement dès lors qu'il traite les données pour ses propres besoins. Tel est le cas, par exemple, lorsque l'application exige un accès à toutes les entrées du carnet d'adresses afin de fournir le service concerné (messagerie instantanée, appels téléphoniques ou vidéo).

Les responsabilités du développeur d'applications seront nettement limitées si aucune donnée à caractère personnel n'est traitée ni/ou accessible en dehors du dispositif, ou si le développeur d'applications a pris les mesures techniques et d'organisation adéquates pour que toutes les données soient anonymisées de manière irréversible et agrégées dans le dispositif même, avant de quitter le dispositif.

Dans tous les cas, si le développeur d'applications obtient l'accès à des informations stockées dans le dispositif, la directive «vie privée et communications électroniques» est également applicable, de sorte que le développeur d'applications est tenu de respecter les dispositions relatives à l'obligation de consentement contenues à l'article 5, paragraphe 3, de cette directive.

Si le développeur d'applications a externalisé une partie ou la totalité du traitement effectif des données à un tiers et que ce tiers assume le rôle de sous-traitant, le développeur d'applications est tenu de respecter l'ensemble des obligations découlant du recours à un sous-traitant. Cela comprend également, le cas échéant, le recours à un fournisseur d'informatique en nuage (par exemple en vue du stockage externe des données)[21].

Dans la mesure où le développeur d'applications autorise des tiers à accéder aux données d'un utilisateur (tels qu'un réseau publicitaire accédant aux données de géolocalisation d'un dispositif dans le cadre de la publicité comportementale), celui-ci doit utiliser les mécanismes appropriés afin de se conformer aux dispositions applicables prévues par le cadre juridique de l'Union européenne. Si le tiers accède aux données stockées dans le dispositif, l'obligation d'obtenir le consentement en toute connaissance de cause visée à l'article 5, paragraphe 3, de la directive «vie privée et communications électroniques», s'applique. En outre, si le tiers traite des données à caractère personnel pour ses propres besoins, il peut également devenir coresponsable du traitement, parallèlement au développeur d'applications, et est donc tenu au respect du principe de limitation de la finalité et au respect des obligations[22] en matière de sécurité pour la partie du traitement dont il détermine les finalités et les moyens. Comme il peut exister différents types d'accords – tant commerciaux que techniques – entre les développeurs d'applications et les tiers, les responsabilités respectives de chaque partie devront être établies au cas par cas en fonction du contexte spécifique dans lequel le traitement est effectué.

---

[21] Voir l'avis 5/2012 du groupe de travail «Article 29» sur l'informatique en nuage (juillet 2012), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_fr.pdf.

[22] Voir l'avis 2/2010 du groupe de travail «Article 29» sur la publicité comportementale en ligne (juin 2010), http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_fr.pdf ainsi que l'avis 1/2010 sur les notions de «responsable du traitement» et de «sous-traitant» (février 2010), http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_fr.pdf

Un développeur d'applications peut utiliser des bibliothèques de tiers avec un logiciel offrant des fonctionnalités communes, comme par exemple une bibliothèque destinée à une plateforme sociale de jeux. Le développeur d'applications doit s'assurer que l'utilisateur est conscient du traitement des données effectué par ces bibliothèques et que, le cas échéant, le traitement de ces données est conforme au cadre juridique de l'Union européenne, y compris, lorsque cela se justifie, en obtenant l'accord de l'utilisateur. À cet effet, les développeurs d'applications doivent empêcher l'utilisation de fonctionnalités cachées à l'utilisateur.

3.3.2 Les fabricants de systèmes d'exploitation et de dispositifs

Les fabricants de systèmes d'exploitation et de dispositifs devraient également être considérés comme responsables du traitement (et, le cas échéant, comme coresponsables du traitement) pour toutes les données à caractère personnel traitées pour leurs propres besoins (bon fonctionnement du dispositif, sécurité, etc.). Cela comprend les données générées par l'utilisateur (par exemple, les coordonnées de l'utilisateur lors de l'inscription), les données générées automatiquement par le dispositif (par exemple, lorsque le dispositif est doté d'une fonctionnalité «appel maison» nécessaire à sa localisation) ou encore les données à caractère personnel traitées par le fabricant du système d'exploitation ou du dispositif à la suite de l'installation ou de l'utilisation d'applications. Si le fabricant du système d'exploitation ou du dispositif fournit des fonctionnalités supplémentaires telles que des services de sauvegarde ou de localisation à distance, il devient également le responsable du traitement pour les données à caractère personnel traitées à cette fin.

Les applications qui exigent un accès aux données de géolocalisation doivent utiliser les services de localisation du système d'exploitation. Lorsqu'une application utilise la géolocalisation, il se peut que le système d'exploitation collecte des données à caractère personnel pour fournir aux applications les informations de géolocalisation et envisage également d'utiliser ces données pour améliorer ses propres services de localisation. Pour cette dernière finalité, le système d'exploitation est responsable du traitement.

Les fabricants du système d'exploitation et du dispositif sont également responsables de l'interface de programmes d'application (API) qui permet le traitement de données à caractère personnel par les applications dans le dispositif intelligent. Le développeur d'applications sera en mesure d'accéder aux options et fonctions que les fabricants du système d'exploitation et du dispositif mettent à disposition à l'aide de l'API. Étant donné que les fabricants du système d'exploitation et du dispositif déterminent les moyens (et la portée) de l'accès aux données à caractère personnel, ils doivent veiller à ce que le développeur d'applications exerce un contrôle à un niveau suffisamment détaillé pour n'autoriser l'accès qu'aux données indispensables au fonctionnement de l'application. Les fabricants du système d'exploitation et du dispositif devraient également faire en sorte que cet accès puisse être révoqué simplement et efficacement.

La notion de «vie privée dès la conception» est un principe important auquel renvoie déjà indirectement la directive sur la protection des données[23] et qui, combiné à la notion de «vie privée par défaut», apparaît plus clairement dans la directive «vie privée et communications électroniques»[24]. Elle exige des fabricants de dispositifs ou des développeurs d'applications qu'ils intègrent la protection des données dès le début de la conception. Le respect de la vie

[23] Voir le considérant 46 et l'article 17.
[24] Voir article 14, paragraphe 3.

privée dès la conception est imposé de manière explicite pour la conception des équipements de télécommunications, conformément à la directive sur les équipements hertziens et les équipements terminaux de télécommunications[25].Les fabricants de systèmes d'exploitation et de dispositifs, ainsi que les magasins d'applications, ont donc une importante responsabilité dans la mesure où ils doivent prévoir les garanties nécessaires à la protection des données à caractère personnel et de la vie privée de l'utilisateur d'applications. Cela comprend, d'une part, la présence de mécanismes adéquats permettant de former l'utilisateur final et de l'informer des actions que les applications peuvent réaliser et des données auxquelles elles peuvent accéder et, d'autre part, la mise à disposition des réglages appropriés permettant à l'utilisateur de modifier les paramètres du traitement[26].

3.3.3 Les magasins d'applications

Les dispositifs intelligents les plus répandus disposent tous de leur propre magasin d'applications et il arrive souvent qu'un système d'exploitation soit étroitement lié à un magasin d'applications donné. Les magasins d'applications traitent souvent le paiement initial et peuvent également prendre en charge les achats intégrés. C'est pourquoi l'inscription de l'utilisateur, avec mention de l'identité, de l'adresse et des données financières, est requise. Ces données (directement) identifiables peuvent être associées à des données sur les achats et les habitudes d'utilisation ainsi qu'à des données lues et générées dans le dispositif (tels que les identifiants uniques). En ce qui concerne le traitement de ces données à caractère personnel, les magasins d'applications seront probablement les responsables du traitement, même s'ils communiquent ces informations en retour aux développeurs de l'application. Lorsque le magasin d'applications traite le téléchargement d'une application d'un utilisateur final, l'historique d'utilisation ou toute autre fonctionnalité comparable permettant de restaurer les applications téléchargées précédemment, ils deviennent également les responsables du traitement pour les données à caractère personnel traitées à cette fin.

Un magasin d'applications enregistre les identifiants de connexion ainsi que l'historique des achats. Il demande également à l'utilisateur de communiquer un numéro de carte de crédit qui sera conservé dans le compte de l'utilisateur. Le magasin d'applications est donc le responsable du traitement pour ces opérations.

Par contre, les sites Internet permettant qu'une application téléchargée soit installée sur un dispositif sans authentification préalable pourraient estimer qu'ils ne traitent pas d'informations à caractère personnel.

[25] Directive 1999/5/CE du 9 mars 1999 concernant les équipements hertziens et les équipements terminaux de télécommunications et la reconnaissance mutuelle de leur conformité, Journal officiel des Communautés européennes n° L 91 du 7.4.1999. L'article 3, paragraphe 3, point c), dispose que la Commission européenne peut décider que les appareils des utilisateurs finaux sont construits de sorte qu'ils comportent des sauvegardes afin d'assurer la protection des données à caractère personnel et de la vie privée des utilisateurs et des abonnés.

[26] Le groupe de travail accueille favorablement les recommandations de la FTC à cet égard, figurant dans le rapport «Mobile Privacy Disclosures» mentionné dans la note 6 supra, notamment à la page 15: «(…) *les plateformes sont en position idéale pour fournir des informations cohérentes tout au long de l'application et sont encouragées en ce sens. Comme le suggèrent les observations émises lors de l'atelier, elles pourraient également envisager de fournir ces informations à différents moments (...).»*

Étant donné leur position, les magasins d'applications ont un rôle important à jouer en permettant aux développeurs d'applications de fournir les informations adéquates sur l'application, y compris sur les types de données susceptibles d'être traitées et sur les finalités du traitement. Les magasins d'applications peuvent imposer ces règles dans le cadre de leur politique d'accès (en recourant à des contrôles ex ante ou ex post). En collaboration avec le fabricant du système d'exploitation, le magasin d'applications peut élaborer un cadre permettant aux développeurs de fournir des avis d'information cohérents et compréhensibles (par exemple sous la forme de symboles représentant certains types d'accès à des données sensorielles) illustrés visiblement dans le catalogue du magasin d'applications.

3.3.4 Les tiers

De nombreux tiers participent au traitement de données lors de l'utilisation d'applications.

Par exemple, de multiples applications gratuites sont financées par des annonces publicitaires, éventuellement, mais pas uniquement, dans le cadre d'une publicité contextuelle ou d'une publicité personnalisée, à l'aide notamment de systèmes de traçage tels que les «cookies traceurs» ou d'autres identifiants présents dans le dispositif. La publicité peut prendre la forme de bannières insérées dans l'application même, d'annonces hors application transmises en modifiant les paramètres de navigation ou en plaçant des icônes sur le bureau mobile, ou encore d'annonces transmises à la suite d'une organisation personnalisée du contenu de l'application (par exemple, dans le cas de résultats de recherche commerciaux).

Dans le domaine des applications, la publicité est généralement proposée par des réseaux publicitaires ou d'autres intermédiaires équivalents éventuellement liés au fabricant du système d'exploitation ou au magasin d'applications, ou faisant éventuellement partie de la même entité. Comme souligné dans l'avis 2/2010[27] du groupe de travail «Article 29», la publicité en ligne implique souvent le traitement de données à caractère personnel telles que définies à l'article 2 de la directive sur la protection des données et interprétées par le groupe de travail «Article 29»[28].

Les fournisseurs de solutions analytiques et de services de communications sont d'autres exemples de tiers. Les fournisseurs de solutions analytiques permettent aux développeurs d'applications d'évaluer l'utilisation, la popularité et la convivialité de leurs applications. Les fournisseurs de services de communications[29] peuvent également jouer un rôle important dans la définition des paramètres par défaut et des mises à jour de sécurité de nombreux dispositifs, et peuvent traiter des données concernant l'utilisation des applications. La personnalisation de ces éléments (le «branding» ou stratégie de marque) pourrait avoir des conséquences sur les mesures techniques et fonctionnelles éventuelles auxquelles l'utilisateur peut avoir recours pour protéger ses données à caractère personnel.

En comparaison avec les développeurs d'applications, les tiers peuvent assumer deux types de rôles: le premier consiste à exécuter des opérations pour le compte du propriétaire de l'application, par exemple en vue d'intégrer des éléments analytiques dans l'application

---

[27] Avis 2/2010 du groupe de travail «Article 29» sur la publicité comportementale en ligne (juin 2010), http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_fr.pdf

[28] Voir également l'interprétation du concept de données à caractère personnel dans l'avis 4/2007 du groupe de travail «Article 29» sur le concept de données à caractère personnel (juin 2007), http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_fr.pdf

[29] Les fournisseurs de services de communications sont également soumis à des obligations en matière de protection des données spécifiques au secteur, qui sortent du champ d'application du présent avis.

même. Dans ce cas, dès lors qu'ils agissent exclusivement pour le compte du développeur d'applications et ne traitent pas les données pour leurs propres besoins et/ou ne partagent pas les données entre plusieurs développeurs, ils assument plutôt une fonction de sous-traitants.

Le second rôle consiste à collecter des informations dans différentes applications afin de proposer des services supplémentaires: fournir des éléments analytiques chiffrés à une plus grande échelle (popularité de l'application, recommandations personnalisées) ou éviter l'affichage multiple d'une même annonce publicitaire sur le dispositif d'un même utilisateur. Lorsque des tiers traitent des données à caractère personnel pour leurs propres besoins, ils agissent en tant que responsables du traitement et sont dès lors tenus de respecter les dispositions applicables au titre de la directive sur la protection des données.[30] Dans le cas de la publicité comportementale, le responsable du traitement doit obtenir le consentement valable de l'utilisateur pour la collecte et le traitement des données à caractère personnel, qui consiste par exemple à analyser et à combiner des données à caractère personnel, à créer et/ou appliquer des profils. Comme expliqué précédemment par le groupe de travail «Article 29» dans son avis 2/2012 sur la publicité comportementale en ligne, les mécanismes de consentement par «opt-in» préalable se prêtent mieux à la manifestation d'un tel consentement.

Une société fournit des métriques aux propriétaires d'applications et aux annonceurs à l'aide de traceurs intégrés dans les applications par le développeur. Les traceurs de cette société peuvent ainsi être installés dans de nombreux dispositifs et applications. Parmi les services proposés, la société renseigne le développeur sur les autres applications de l'utilisateur, par la collecte d'un identifiant unique. Elle définit les moyens (en l'occurrence, les traceurs) et les finalités de ses outils avant de les proposer aux développeurs d'applications, aux annonceurs et à d'autres parties, agissant ainsi en tant que responsable du traitement.

Dans la mesure où des tiers accèdent à des informations ou stockent des informations dans le dispositif intelligent, ils sont tenus de respecter l'obligation de consentement visée à l'article 5, paragraphe 3, de la directive «vie privée et communications électroniques».

Dans ce contexte, il importe de noter que l'utilisateur a généralement peu de possibilités d'installer dans son dispositif intelligent des logiciels susceptibles de contrôler le traitement de données à caractère personnel comme cela est courant dans un environnement de bureau «web». Comme solution de rechange à l'utilisation de cookies HTTP, les tiers accèdent souvent aux identifiants uniques afin de viser certains (groupes d') utilisateurs et de leur proposer des services ciblés, y compris des annonces publicitaires. Comme la plupart de ces identifiants ne peuvent être supprimés ou modifiés par les utilisateurs (tels que l'IMEI, l'IMSI, le MSISDN[31] et d'autres identifiants uniques et spécifiques intégrés au dispositif par le système d'exploitation), les tiers ont la possibilité de traiter des quantités considérables de données à caractère personnel en l'absence de tout contrôle de la part de l'utilisateur final.

[30] Avis 2/2010 du groupe de travail «Article 29» sur la publicité comportementale en ligne, p. 12-13.
[31] Réseau numérique à intégration de services pour les stations mobiles

3.4 Fondements juridiques

Le traitement de données à caractère personnel ne peut être effectué que s'il repose sur une base juridique, telle qu'énoncée à l'article 7 de la directive sur la protection des données. L'article 7 distingue six cas dans lesquels le traitement de données peut être légalement effectué. La personne concernée a indubitablement donné son consentement et le traitement est nécessaire à: l'exécution d'un contrat avec la personne concernée, à la sauvegarde de l'intérêt vital de la personne concernée, au respect d'une obligation légale, à l'exécution d'une mission d'intérêt public (dans le cas d'autorités publiques) et à la réalisation de l'intérêt légitime (de l'entreprise).

En ce qui concerne le stockage d'informations, ou l'obtention de l'accès à des informations déjà stockées dans le dispositif intelligent, l'article 5, paragraphe 3, de la directive «vie privée et communications électroniques» (c.-à-d. l'obligation de consentement pour le placement ou la récupération d'informations dans un dispositif) impose une limitation/restriction plus détaillée des fondements juridiques susceptibles d'être pris en compte.

3.4.1 Consentement préalable au stockage et au traitement de données à caractère personnel

Dans le cas des applications, le consentement constitue le principal fondement juridique applicable. Lors de l'installation d'une application, des informations sont placées dans le dispositif de l'utilisateur final. De nombreuses applications accèdent également à des données stockées dans le dispositif (contacts du carnet d'adresses, photos, vidéos et autres documents personnels). Dans tous ces cas, l'article 5, paragraphe 3, de la directive «vie privée et communications électroniques» dispose que le consentement de l'utilisateur doit être donné, après avoir reçu une information claire et complète, préalablement au placement et à la récupération d'informations dans le dispositif.

Il convient de noter que le consentement requis pour placer ou lire une quelconque information dans un dispositif se distingue du consentement nécessaire à l'obtention d'une base juridique autorisant le traitement de différents types de données à caractère personnel. Bien que ces deux obligations de consentement soient simultanément applicables, fondées chacune sur une base juridique différente, elles sont toutes deux soumises aux conditions suivantes: le consentement doit être libre, spécifique et informé (conformément à l'article 2, point h), de la directive sur la protection des données). C'est pourquoi les deux types de consentement peuvent être fusionnés dans la pratique, soit au cours de l'installation, soit avant le début de la collecte des données à caractère personnel dans le dispositif, pour autant que l'utilisateur ait pris conscience, sans aucune ambigüité, de l'autorisation qu'il s'apprête à accorder.

De nombreux magasins d'applications offrent aux développeurs d'applications la possibilité d'informer l'utilisateur final des caractéristiques de base d'une application préalablement à l'installation, et de demander l'autorisation de l'utilisateur avant le téléchargement et l'installation de l'application (c.-à-d. le bouton «Installer»). Alors qu'une telle action peut, dans certaines circonstances, satisfaire à l'obligation de consentement visée à l'article 5, paragraphe 3, il est improbable que les informations communiquées suffisent à faire de cette action un acte de consentement valable pour le traitement des données à caractère personnel.

Ce sujet a été abordé précédemment dans l'avis 15/2011 du groupe de travail «Article 29» sur la définition du consentement[32].

Dans le cadre des dispositifs intelligents, «libre» signifie qu'un utilisateur doit avoir le choix d'accepter ou de refuser le traitement de ses données à caractère personnel. Si une application doit traiter ce type de données, un utilisateur doit donc être libre d'accepter ou de refuser. L'utilisateur ne peut se trouver face à un écran proposant uniquement l'option «Oui, j'accepte» afin de finaliser l'installation. Une option «Annuler» ou toute autre option permettant d'arrêter l'installation doit être proposée.

«Informé» signifie que la personne concernée doit disposer des informations nécessaires afin de se forger une opinion exacte[33]. Pour éviter tout risque d'ambigüité, ces informations doivent être disponibles avant que les données à caractère personnel ne soient traitées. Cela inclut le traitement de données susceptible d'être effectué au cours de l'installation, par exemple, à des fins de débogage ou de traçage. Le contenu et la forme de ces informations seront explicités au point 3.7 du présent avis.

«Spécifique» signifie que la manifestation de volonté doit concerner le traitement d'une donnée particulière ou d'une catégorie limitée de données. C'est pourquoi le simple fait de cliquer sur un bouton «Installer» ne peut être considéré comme un consentement valable pour le traitement de données à caractère personnel dans la mesure où un consentement ne peut s'exprimer par une autorisation formulée de manière générale. Dans certains cas, l'utilisateur est en mesure de donner un consentement détaillé, lorsque le consentement est demandé pour chaque type de données auquel l'application est sur le point d'accéder[34].Une telle approche permet de satisfaire à deux dispositions juridiques importantes: d'une part, l'obligation d'informer de manière adéquate l'utilisateur des aspects essentiels du service proposé et, d'autre part, la demande de consentement spécifique pour chacun de ces services[35].L'autre approche adoptée par les développeurs d'applications, invitant l'utilisateur à accepter une longue énumération de conditions générales et/ou leur politique de confidentialité, ne peut s'apparenter à un consentement spécifique[36].

La notion de «spécifique» concerne également la pratique consistant à tracer le comportement des utilisateurs et utilisée par des annonceurs ou toute autre partie tierce. Les paramètres par défaut proposés par les systèmes d'exploitation et les applications doivent être conçus de manière à empêcher tout traçage, afin de permettre à l'utilisateur de donner son consentement

---

[32] Avis 15/2011 du groupe de travail «Article 29» sur la définition du consentement (juillet 2011), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_fr.pdf

[33] Idem, p. 21.

[34] Un consentement détaillé signifie que les personnes peuvent contrôler de manière plus fine (spécifique) les fonctions de traitement de données à caractère personnel proposées par l'application qu'elles souhaitent activer.

[35] La nécessité d'un consentement détaillé est également reconnue de manière explicite par le personnel de la FTC dans son rapport le plus récent (voir note 6 supra), p. 15-16: «(…) *les plateformes devraient envisager de fournir des informations au moment opportun et d'obtenir le consentement explicite pour la collecte de contenus que de nombreux consommateurs jugeraient sensibles dans de nombreux contextes, tels que des photos, des contacts, des entrées de calendrier, ou encore l'enregistrement de contenus audio ou vidéo*.»

[36] Idem, p 34-35: «*Un consentement général dépourvu d'une indication précise sur la finalité du traitement que la personne concernée accepte ne satisfait pas à cette obligation. Cela signifie que les informations relatives à la finalité du traitement ne doivent pas être incluses dans les dispositions générales mais dans une clause de consentement séparée.*»

spécifique pour ce type de traitement. Ces paramètres par défaut ne doivent pas pouvoir être contournés par des tiers, comme c'est souvent le cas aujourd'hui avec la fonctionnalité «ne pas suivre» (*do not track*) embarquée au sein des navigateurs.

Exemples de consentement spécifique

Une application fournit des informations sur les restaurants situés à proximité. Préalablement à l'installation, le développeur d'applications doit demander le consentement de l'utilisateur. Pour accéder aux données de géolocalisation, le développeur d'applications doit demander un consentement séparé, par exemple au cours de l'installation ou avant l'accès aux données de géolocalisation.
«Spécifique» signifie que le consentement doit être limité à la finalité spécifique qui consiste ici à informer l'utilisateur des restaurants situés à proximité. L'accès aux données de localisation du dispositif ne peut donc s'effectuer que lorsque l'utilisateur recourt à l'application à cette fin. Le consentement de l'utilisateur en vue du traitement des données de géolocalisation n'autorise pas l'application à collecter en continu les données de localisation du dispositif. Cet autre traitement impliquerait des informations supplémentaires et un consentement séparé.

De même, pour qu'une application de communication puisse accéder à la liste des contacts, l'utilisateur doit être en mesure de sélectionner les contacts avec lesquels il souhaite communiquer, plutôt que de devoir accorder l'accès à l'ensemble du carnet d'adresses (y compris aux coordonnées de personnes qui n'utilisent pas ce service et qui ne peuvent dès lors avoir donné leur consentement pour le traitement des données les concernant).

Il convient de noter toutefois que, même si le consentement remplit les trois conditions décrites ci-dessus, il n'autorise pas pour autant un traitement déloyal et illicite. Si la finalité du traitement des données est excessive et/ou disproportionnée, et même si l'utilisateur a donné son consentement, le développeur d'applications ne peut se prévaloir d'un fondement juridique valable et ne respecte pas dans ce cas la directive sur la protection des données.

Exemple de traitement de données excessif et illicite

Une application de type «alarme» propose en option la possibilité pour l'utilisateur d'exécuter une commande vocale afin d'interrompre ou de suspendre l'alarme. Dans cet exemple, l'accord d'enregistrement se limite à la durée de l'alarme. Tout contrôle ou enregistrement audio en dehors du fonctionnement de l'alarme serait considéré comme excessif et illicite.

Dans le cas d'applications installées par défaut dans le dispositif (avant que l'utilisateur n'en devienne propriétaire) ou de traitements effectués par le système d'exploitation exigeant un consentement comme base juridique, les responsables du traitement doivent examiner attentivement si ce consentement est réellement valable. Dans de nombreux cas, un mécanisme de consentement séparé devrait être envisagé, par exemple lors de la première exécution de l'application, de façon à donner au responsable du traitement la possibilité suffisante d'informer de manière complète l'utilisateur final. Lorsqu'il s'agit de catégories particulières de données, telles que définies à l'article 8 de la directive sur la protection des données, le consentement doit être explicite.

Dernière précision mais non des moindres, l'utilisateur doit avoir la possibilité de retirer son consentement de manière simple et efficace. Cette question sera traitée plus en profondeur au point 3.8 du présent avis.

3.4.2 Les fondements juridiques pour le traitement de données durant l'utilisation d'une application

Comme expliqué ci-dessus, le consentement constitue le fondement juridique autorisant le développeur d'applications à lire et/ou écrire des informations en toute légalité et, par conséquent, à traiter des données à caractère personnel. Dans une phase ultérieure, au cours de l'utilisation de l'application, le développeur d'applications peut invoquer d'autres fondements juridiques pour d'autres types de traitement, pour autant que cela n'implique pas le traitement de données sensibles à caractère personnel.

Ces fondements juridiques peuvent être nécessaires à l'exécution d'un contrat avec la personne concernée ou à la réalisation des intérêts légitimes (de l'entreprise), conformément à l'article 7, points b) et f), de la directive sur la protection des données.

Ces fondements juridiques se limitent au traitement de données à caractère personnel non sensibles d'un utilisateur spécifique, et ne peuvent être invoqués que dans la mesure où un traitement de données particulier est strictement nécessaire à la réalisation du service souhaité et, conformément à l'article 7, point f), à condition que ne prévalent pas l'intérêt ou les droits et libertés fondamentaux de la personne concernée.

Exemples de fondement juridique contractuel

Un utilisateur donne son accord pour l'installation d'une application de services bancaires mobiles. Afin de répondre à une demande d'exécution de paiement, la banque n'est pas tenue de demander le consentement séparé de l'utilisateur pour communiquer le nom et le numéro de compte bancaire de ce dernier au bénéficiaire du paiement. Cette information est strictement nécessaire à l'exécution du contrat avec cet utilisateur spécifique et, dès lors, la banque peut invoquer le fondement juridique visé à l'article 7, point b), de la directive sur la protection des données. Ce même raisonnement s'applique aux applications de communication; lorsque celles-ci transmettent des informations essentielles telles qu'un nom de compte, une adresse électronique ou un numéro de téléphone à une autre personne avec laquelle l'utilisateur souhaite communiquer, cette transmission est naturellement nécessaire à l'exécution du contrat.

3.5 Limitation de la finalité et minimisation des données

Les principes fondamentaux qui sous-tendent la directive sur la protection des données sont la limitation de la finalité et la minimisation des données. La limitation de la finalité permet à l'utilisateur de choisir délibérément de confier ses données à caractère personnel à une autre partie étant donné qu'il saura de quelle manière ses données sont utilisées et qu'il pourra se fier à la description de la finalité restreinte pour comprendre à quelles fins ses données seront utilisées. Les finalités du traitement doivent dès lors être bien définies et compréhensibles pour un utilisateur moyen ne disposant pas de connaissances juridiques ou techniques approfondies.

Dans le même temps, la limitation de la finalité implique que les développeurs d'applications aient un bon aperçu de leur projet préalablement à la collecte des données à caractère personnel provenant de l'utilisateur. Ces données ne peuvent être traitées que loyalement et licitement (conformément à l'article 6, paragraphe 1, point a), de la directive sur la protection des données) et les finalités doivent être définies préalablement au traitement des données.

Le principe de limitation de la finalité exclut des modifications inopinées dans les conditions d'utilisation essentielles régissant le traitement.

Par exemple, dans une application dont la finalité initiale est de permettre aux utilisateurs de communiquer par courriel, le développeur décide de modifier son mode de fonctionnement et fusionne les adresses électroniques de ses utilisateurs avec les numéros de téléphone des utilisateurs d'une autre application. Les responsables du traitement respectifs devraient dans ce cas contacter individuellement chaque utilisateur et demander son consentement préalable et explicite autorisant la nouvelle finalité du traitement des données à caractère personnel les concernant.

La limitation de la finalité va de pair avec le principe de minimisation des données. Afin de prévenir tout traitement de données superflu et potentiellement illicite, les développeurs d'applications doivent définir scrupuleusement les données qui seront strictement nécessaires à la réalisation de la fonctionnalité souhaitée.

Étant donné que les applications peuvent obtenir un accès à un grand nombre de fonctionnalités présentes dans le dispositif, celles-ci sont en mesure d'exécuter de nombreuses opérations telles que l'envoi de SMS furtifs ou l'accès aux images et aux entrées du carnet d'adresses. De nombreux magasins d'applications prennent en charge des mises à jour (semi) automatiques dans lesquelles le développeur d'applications peut intégrer de nouvelles fonctionnalités et les rendre accessibles avec peu ou pas d'interaction de la part de l'utilisateur final.

Le groupe de travail souligne à ce stade que les tiers obtenant un accès aux données de l'utilisateur par le biais des applications sont tenus de respecter les principes de limitation de la finalité et de minimisation des données. Les identifiants uniques des dispositifs, souvent impossibles à modifier, ne devraient pas être utilisés à des fins publicitaires (annonces ciblées selon les intérêts) et/ou analytiques, étant donné l'incapacité pour l'utilisateur de révoquer son consentement. Les développeurs d'applications devraient veiller à ce qu'aucun détournement d'utilisation ne se produise en ne modifiant pas le traitement lors du passage d'une application à une autre sans fournir à l'utilisateur final les informations appropriées et la possibilité de renoncer soit au traitement, soit au service tout entier. L'utilisateur devrait également disposer des moyens techniques qui lui permettent de vérifier les finalités annoncées, en ayant la possibilité de comparer le volume de trafic sortant par application au trafic généré par lui-même.

Les informations et les contrôles de l'utilisateur sont les principaux garants du respect des principes de minimisation des données et de limitation de la finalité.

L'accès, à l'aide des API, aux données sous-jacentes présentes dans le dispositif offre aux fabricants de systèmes d'exploitation et de dispositifs, ainsi qu'aux magasins d'applications, la possibilité d'imposer des règles spécifiques et de communiquer les informations appropriées à l'utilisateur final. Par exemple, les fabricants de systèmes d'exploitation et de dispositifs devraient proposer des API assorties de contrôles précis permettant de différencier les divers types de données et veiller à ce que les développeurs d'applications puissent demander l'accès exclusivement aux données strictement nécessaires à la fonctionnalité (licite) de leurs applications. Les types de données demandés par le développeur d'applications peuvent ainsi être clairement affichés dans le magasin d'applications afin d'informer l'utilisateur préalablement à l'installation.

À cet égard, le contrôle de l'accès aux données stockées dans le dispositif repose sur différents mécanismes:

a. les fabricants des systèmes d'exploitation et des dispositifs, ainsi que les magasins d'applications, définissent les **règles** en vigueur pour toutes les applications que les développeurs souhaitent placer dans les magasins: ces derniers sont tenus de respecter ces règles au risque de voir leurs applications rejetées par lesdits magasins[37];
b. les **API** du système d'exploitation définissent des méthodes normalisées pour accéder aux données stockées dans le téléphone et accessibles aux applications. Elles ont également une incidence sur la collecte des données au niveau du serveur;
c. **contrôles ex ante** – c.-à-d. les contrôles réalisés avant l'installation d'une application;[38]
d. **contrôles ex post** - c.-à-d. les contrôles réalisés après l'installation d'une application.

3.6 Sécurité

Selon l'article 17 de la directive sur la protection des données, les responsables du traitement et les sous-traitants doivent prendre les mesures techniques et d'organisation nécessaires pour protéger les données à caractère personnel qu'ils traitent. Par conséquent, les mesures doivent être prises par l'ensemble des intervenants recensés au point 3.3, chacun en fonction de ses propres rôle et responsabilité.

Le respect de l'obligation de sécurité poursuit un objectif double. Il permet d'une part à l'utilisateur de contrôler ses données de manière plus stricte et contribue, d'autre part, à augmenter le niveau de confiance dans les entités qui, dans la pratique, traitent les données de l'utilisateur.

Afin de s'acquitter de leurs obligations de sécurité respectives en tant que responsables du traitement, les développeurs et les magasins d'applications, les fabricants de systèmes d'exploitation et de dispositifs ainsi que les tiers doivent tenir compte des principes de protection de la vie privée dès la conception et de protection de la vie privée par défaut. Cela implique une appréciation continue des risques existants et futurs en matière de protection des données, ainsi que la mise en œuvre et l'évaluation de mesures d'atténuation efficaces, parmi lesquelles la minimisation des données.

Les développeurs d'applications

Dans le domaine de la sécurité des applications mobiles, de nombreuses lignes directrices accessibles au public ont déjà été publiées par les fabricants de systèmes d'exploitation et de

[37] Les appareils débridés permettent l'installation d'applications en dehors du circuit officiel; les appareils Android permettent également l'installation d'applications en provenance d'autres sources.
[38] Il est à noter que dans certains cas particuliers, les applications sont préinstallées.

dispositifs ainsi que par des parties tierces indépendantes (par exemple, les lignes directrices de l'ENISA[39]).

L'examen de toutes les bonnes pratiques en matière de sécurité concernant le développement d'applications ne rentre pas dans le champ d'application du présent avis; toutefois, le groupe de travail saisit cette opportunité pour passer en revue les pratiques susceptibles de nuire gravement aux droits fondamentaux des utilisateurs d'applications.

Il est important de décider, préalablement à la conception d'une application, du lieu de stockage des données. Dans certains cas, les données relatives à l'utilisateur sont stockées dans le dispositif mais il se peut également que les développeurs d'applications utilisent une architecture client-serveur. Cela signifie que les données à caractère personnel sont transférées ou copiées vers les systèmes du fournisseur de services. Le stockage et le traitement des données dans le dispositif même offrent à l'utilisateur final le maximum de contrôle sur ces données, par exemple en lui permettant de supprimer les données pour le traitement desquelles il a retiré son consentement. Cependant, le stockage à distance et en toute sécurité des données peut se révéler utile pour la récupération des données en cas de perte ou de vol du dispositif. Des solutions intermédiaires sont également envisageables.

Les développeurs d'applications doivent élaborer pour leurs logiciels des politiques de développement et de distribution claires. Les fabricants de systèmes d'exploitation et de dispositifs ont également un rôle à jouer en encourageant des traitements sécurisés par les applications, qui seront détaillés ci-dessous. Ensuite, les développeurs et les magasins d'applications doivent concevoir et mettre en place un environnement privilégiant la sécurité, avec des outils empêchant la diffusion d'applications malveillantes et permettant l'installation et la désinstallation aisées de chaque application.

Les bonnes pratiques susceptibles d'être utilisées lors de la conception d'une application comprennent, entre autres, la réduction du nombre de lignes de code et la simplification du code, ainsi que la mise en place de contrôles permettant d'éviter que des données ne soient accidentellement transférées ou compromises. En outre, toutes les entrées devraient être validées afin de prévenir un débordement de la mémoire tampon ou des attaques par injection. D'autres mécanismes de sécurité qui méritent d'être mentionnés comprennent des stratégies adéquates pour la gestion des correctifs de sécurité ainsi que la réalisation d'audits réguliers et indépendants de la sécurité du système. De plus, les critères de conception des applications devraient inclure l'application du principe du «moindre privilège par défaut», en vertu duquel les applications ne peuvent accéder qu'aux données dont elles ont réellement besoin pour garantir à l'utilisateur l'accessibilité d'une fonctionnalité. Les développeurs et les magasins d'applications devraient également encourager les utilisateurs, par des messages d'avertissement, à compléter ces bonnes pratiques de conception par d'excellentes pratiques d'utilisation, comme la mise à niveau des applications vers les dernières versions disponibles, et les encourager, par des rappels, à ne pas utiliser un mot de passe identique pour différents services.

Au cours de la phase de conception de l'application, les développeurs doivent également prendre les mesures visant à empêcher l'accès non autorisé à des données à caractère

[39] ENISA, «Orientation pour le développement sûr de téléphones intelligents»: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-applications/smartphone-security-1/smartphone-secure-development-guidelines.

personnel, en garantissant la protection des données, tant durant le transfert que pendant le stockage, selon les cas.

Les applications mobiles devraient être exécutées dans des emplacements spécifiques au cœur même de la mémoire des dispositifs (des «sandbox»[40]), afin de limiter les conséquences des applications ou des logiciels malveillants. En étroite collaboration avec le fabricant du système d'exploitation et/ou le magasin d'applications, les développeurs doivent utiliser les mécanismes disponibles permettant à l'utilisateur de repérer les données en cours de traitement et les applications concernées, et de pouvoir, au choix, activer ou désactiver les autorisations. L'utilisation de fonctionnalités cachées devrait être prohibée.

Les développeurs d'applications doivent être très attentifs aux méthodes envisagées pour l'identification et l'authentification de l'utilisateur. Ils ne devraient pas utiliser les identifiants permanents (spécifiques au dispositif) mais recourir au contraire à des identifiants spécifiques à l'application et à faible valeur entropique, ou à des identifiants de dispositif qui soient temporaires, de manière à éviter le traçage des utilisateurs dans le temps. Des mécanismes d'authentification respectueux de la vie privée devraient être envisagés. Lors de l'authentification de l'utilisateur, les développeurs d'applications doivent accorder une attention particulière à la gestion des identités et des mots de passe. Ces derniers doivent être stockés de manière encryptée et sûre, en tant que valeurs de hachage cryptographique avec chiffrement par clé. La mise à disposition de tests permettant à l'utilisateur de vérifier la robustesse des mots de passe choisis est également une technique utile pour encourager l'utilisation de mots de passe plus adaptés (vérification de l'entropie). En fonction des besoins (l'accès à des données sensibles mais également l'accès à des ressources payantes), une nouvelle authentification pourrait être envisagée, également à l'aide de facteurs multiples et de canaux différents (par exemple, un code d'accès envoyé par SMS) et/ou de données d'authentification liées à l'utilisateur final (plutôt qu'au dispositif). De même, lors de la sélection d'identifiants de session, des chaînes imprévisibles devraient être utilisées, éventuellement en combinaison avec des informations contextuelles telles que la date et l'heure, mais également l'adresse IP ou des données de géolocalisation.

Les développeurs d'applications devraient également être conscients des exigences contenues dans la directive «vie privée et communications électroniques» concernant la violation des données à caractère personnel et l'obligation d'informer les utilisateurs de manière proactive. Bien que ces exigences ne s'appliquent actuellement qu'aux fournisseurs de services de communications électroniques accessibles au public, il est probable que ces obligations soient étendues à tous les responsables du traitement (et aux sous-traitants) par le biais du futur règlement relatif à la protection des données, qui s'inspire des propositions de la Commission (COM 2012/0011/COD). Ces nouvelles dispositions renforcent encore la nécessité d'élaborer et d'évaluer en continu un «plan de sécurité» détaillé couvrant la collecte, le stockage et le traitement de toutes les données à caractère personnel, afin de prévenir la violation de ces dernières et d'éviter les sanctions financières lourdes envisagées dans de tels cas. Le plan de sécurité, entre autres, doit également prévoir la gestion de la vulnérabilité ainsi que la mise à disposition, au moment opportun et en toute sécurité, de corrections de bogues fiables.

La responsabilité des développeurs d'applications à l'égard de la sécurité de leurs produits ne se limite pas à la mise sur le marché d'une version fonctionnelle. Étant donné que les

[40] Un «sandbox» est un mécanisme de sécurité permettant de séparer des programmes en cours d'exécution.

applications peuvent, comme tout produit logiciel, connaître des failles au niveau de la sécurité et présenter des vulnérabilités, les développeurs doivent concevoir les corrections correspondantes et les fournir aux autres intervenants qui pourront à leur tour les mettre à la disposition des utilisateurs, ou s'en charger eux-mêmes.

Les magasins d'applications

Les magasins d'applications, intermédiaires importants entre l'utilisateur final et les développeurs d'applications, devraient soumettre les applications à un certain nombre de contrôles solides et efficaces avant d'autoriser leur mise sur le marché. Ils devraient fournir des informations sur les vérifications auxquelles ils procèdent dans la pratique et préciser le type de contrôles de conformité réalisés en matière de protection des données.

Bien que cette mesure ne soit pas totalement efficace contre la diffusion d'applications malveillantes, les statistiques montrent que cette pratique réduit sensiblement l'apparition de fonctionnalités malveillantes dans les magasins d'applications «officiels».[41] Pour faire face au nombre élevé d'applications proposées chaque jour, ce processus pourrait bénéficier d'outils d'analyse automatique et de la mise en place de canaux d'échange d'informations entre les experts en sécurité et les professionnels de la programmation. Il devrait également pouvoir s'appuyer sur des procédures et des politiques efficaces permettant la gestion des problématiques soulevées.

Outre le contrôle dont elles font l'objet avant leur acceptation dans le magasin, les applications devraient être soumises également à une évaluation du public (mécanisme de réputation). Les applications ne devraient pas être jugées par les utilisateurs uniquement en fonction de leur aspect «sympa» mais également sur la base de leurs fonctionnalités, et plus particulièrement de leurs mécanismes de sécurité et de protection de la vie privée. De même, les mécanismes de réputation devraient être conçus afin de prévenir toute fausse évaluation. Les mécanismes d'acceptation et de réputation pour les applications peuvent également se révéler positifs dans la mesure où ils contribuent à instaurer un climat de confiance mutuelle entre les diverses entités, notamment lorsque l'échange des données passe par une longue chaîne de parties tierces.

Les magasins d'applications ont souvent mis en place une méthode permettant de désinstaller à distance des applications malveillantes ou douteuses. Ce mécanisme, s'il n'est pas correctement conçu, pourrait priver l'utilisateur de la possibilité d'exercer un contrôle plus rigoureux de ses données. Dans le cas des magasins d'applications, un outil de désinstallation à distance respectueux de la vie privée devrait reposer sur la communication des informations et le consentement de l'utilisateur. En outre, d'un point de vue plus pratique, des canaux de communication pour le retour d'information devraient être proposés aux utilisateurs pour que ces derniers fassent part des problèmes de sécurité rencontrés dans leurs applications et de l'efficacité de chaque procédure de suppression à distance.

Tout comme les développeurs, les magasins d'applications devraient être conscients des futures obligations concernant la notification de toute violation de données à caractère personnel, et devraient collaborer étroitement avec les développeurs d'applications afin de prévenir de telles violations.

---

[41] *«Hey, You, Get Off of My Market: Detecting Malicious Apps in Official and Alternative Android Markets»*, Y Zhou et al., Symposium 2012 sur la sécurité des réseaux et des systèmes distribués (NDSS)

Les fabricants de systèmes d'exploitation et de dispositifs

Les fabricants de systèmes d'exploitation et de dispositifs jouent également un rôle important dans la définition des normes minimales et des bonnes pratiques en vigueur chez les développeurs d'applications, non seulement au niveau de la sécurité du logiciel sous-jacent et des API, mais également en ce qui concerne les outils, les lignes directrices et le matériel de référence que ceux-ci mettent à disposition. Les fabricants de systèmes d'exploitation et de dispositifs devraient proposer des algorithmes de chiffrement solides et courants, et permettre la prise en charge de longueurs de clé appropriées. Ils pourraient également mettre à la disposition des développeurs d'applications des mécanismes d'authentification solides et sûrs (par exemple, l'utilisation de certificats signés par des autorités de certification de confiance afin de vérifier l'autorisation d'une ressource à distance). Cela éviterait également aux développeurs d'applications de devoir concevoir des mécanismes d'authentification propriétaires. Dans la pratique, ces procédures sont rarement mises en place, ce qui peut constituer une vulnérabilité sérieuse[42].

L'accès et le traitement des données à caractère personnel par les applications devraient être gérés par des classes et des méthodes intégrées dans les API et garantissant des protections et des vérifications correctes. Les fabricants de systèmes d'exploitation et de dispositifs devraient veiller à ce que les méthodes et les fonctions autorisant l'accès aux données à caractère personnel comprennent des fonctionnalités visant à mettre en place des requêtes de consentement détaillé. De même, des mesures devraient être prises pour exclure ou limiter l'accès aux données à caractère personnel à l'aide de fonctions bas niveau ou d'autres moyens susceptibles de contourner les contrôles et protections intégrés dans les API.

Les fabricants de systèmes d'exploitation et de dispositifs doivent également concevoir dans les dispositifs des pistes d'audit claires de sorte que l'utilisateur final puisse repérer facilement les applications accédant aux données présentes dans son dispositif.

Toutes les parties doivent réagir rapidement et de manière opportune aux vulnérabilités en matière de sécurité afin que l'utilisateur final ne soit pas inutilement exposé aux failles de sécurité. Malheureusement, certains fabricants de systèmes d'exploitation et de dispositifs (ainsi que certains opérateurs de télécommunications lorsqu'ils distribuent des appareils siglés) ne prennent plus en charge à long terme certaines versions du système d'exploitation, ce qui laisse l'utilisateur démuni face à des vulnérabilités pourtant bien connues. Les fabricants de systèmes d'exploitation et de dispositifs, ainsi que les développeurs d'applications, doivent dès le départ communiquer à l'utilisateur final la durée pendant laquelle il peut attendre des mises à jour de sécurité régulières. Ils devraient également informer les utilisateurs, dans les meilleurs délais, lorsque la correction d'un problème de sécurité exige l'installation d'une mise à jour.

---

[42] Il a été observé récemment que l'absence d'indicateurs de sécurité visuels lors de l'utilisation de protocoles SSL/TLS et le recours inapproprié à ces derniers peuvent être exploités pour lancer des attaques de type HDM (attaques de l'homme du milieu). Selon des recherches récentes, la base installée cumulée d'applications présentant des vulnérabilités confirmées face aux attaques HDM compte plusieurs millions d'utilisateurs. "*Why Eve and Mallory Love Android: An Analysis of Android SSL (In)Security"*, Bernd Freisleben et Matthew Smith, 19e conférence sur la sécurité informatique et des communications, organisée en 2012 par l'association ACM.

Les tiers
Les éléments de sécurité et les principes ci-dessus doivent être également appliqués par les tiers dès lors qu'ils collectent et traitent des données à caractère personnel pour leurs propres besoins. C'est notamment le cas des annonceurs et des fournisseurs de solutions analytiques. Cela inclut la transmission sécurisée et le stockage crypté d'identifiants uniques pour les dispositifs et les utilisateurs d'applications, ainsi que d'autres données à caractère personnel.

3.7 Informations

3.7.1 L'obligation d'informer et le contenu requis

Conformément à l'article 10 de la directive sur la protection des données, toutes les personnes concernées ont le droit de connaître l'identité du responsable du traitement des données à caractère personnel les concernant. En outre, dans le cadre des applications, l'utilisateur final a le droit de connaître la nature des données à caractère personnel objet du traitement ainsi que la finalité escomptée de leur utilisation. Si les données à caractère personnel de l'utilisateur sont collectées auprès d'autres acteurs de l'écosystème applicatif (comme décrit au point 3.3 du présent avis), l'utilisateur final, sur la base de l'article 11 de la directive sur la protection des données, a néanmoins le droit d'être informé du traitement de ces données, conformément à ce qui a été décrit. C'est pourquoi, en cas de traitement de données à caractère personnel, le responsable du traitement concerné est tenu de fournir aux utilisateurs potentiels au moins les informations suivantes:

— l'identité et les coordonnées du responsable du traitement;
— les catégories précises des données à caractère personnel que le développeur d'applications entend collecter et traiter;
— la finalité (les objectifs précis du traitement);
— la confirmation d'une transmission éventuelle des données à des tiers;
— la manière dont l'utilisateur peut exercer ses droits dans le cas d'un retrait de consentement ou de suppression de données.

La disponibilité des informations relatives au traitement de données à caractère personnel est essentielle pour l'obtention du consentement de l'utilisateur. Le consentement ne sera valable que si la personne a été informée au départ des principaux éléments du traitement. La communication de ces informations après le début du traitement des données à caractère personnel (qui commence souvent pendant l'installation de l'application) n'est pas jugé suffisante et est juridiquement sans valeur. En accord avec le rapport du personnel de la FTC, le groupe de travail souligne la nécessité de fournir les informations au moment opportun pour les consommateurs, juste avant la collecte de ces informations par les applications. Il est particulièrement important d'être informé des données en cours de traitement dans la mesure où les applications ont généralement un accès peu restreint aux capteurs et aux structures de données présentes dans le dispositif alors que, dans de nombreux cas, un tel accès ne semble pas intrinsèquement évident. Des informations adéquates sont également d'une importance vitale lorsque l'application traite des catégories particulières de données à caractère personnel, telles que les conditions de santé, les convictions politiques, l'orientation sexuelle, etc. Enfin, le développeur d'applications devrait distinguer clairement les informations obligatoires de celles facultatives, et le système devrait permettre à l'utilisateur de refuser l'accès aux informations facultatives en sélectionnant des options par défaut privilégiant le respect de la vie privée.

En ce qui concerne l'identité du responsable du traitement, l'utilisateur doit savoir qui est juridiquement responsable du traitement de ses données à caractère personnel et comment ce dernier peut être contacté. Dans le cas contraire, il ne sera pas en mesure d'exercer ses droits, comme par exemple le droit d'accéder aux données personnelles stockées (à distance). Étant donné le caractère fragmenté de l'environnement applicatif, il est essentiel que chaque application dispose d'un seul point de contact, qui sera responsable de l'ensemble du traitement effectué à l'aide de cette application. Il n'appartient pas à l'utilisateur final de devoir rechercher les relations existant entre le développeur d'une application et les autres parties associées au traitement des données à caractère personnel dans le cadre de cette application.

En ce qui concerne la/les finalité(s), l'utilisateur final doit être correctement informé de la nature et de la finalité des données collectées à son sujet. L'utilisateur devrait être également averti dans un langage clair et simple du fait que les données sont susceptibles d'être réutilisées par d'autres parties et, le cas échéant, des finalités envisagées. Des finalités vagues telles que «l'innovation des produits» ne constituent pas une information adéquate à l'intention des utilisateurs. Il devrait être précisé en termes simples si l'utilisateur sera invité à autoriser le partage des données avec des tiers à des fins publicitaires et/ou analytiques. Les magasins d'applications ont comme importante responsabilité de veiller à ce que ces informations soient disponibles et facilement accessibles pour chaque application.

Les magasins d'applications ont comme autre responsabilité importante de garantir des informations adéquates. L'utilisation de symboles visuels ou d'icônes concernant l'utilisation des données est vivement recommandée afin que les utilisateurs soient conscients des diverses catégories de traitement de données.

Outre les informations minimales énumérées ci-dessus, nécessaires à l'obtention du consentement de l'utilisateur de l'application, le groupe de travail recommande instamment, en vue du traitement loyal des données à caractère personnel, que les responsables du traitement fournissent également à l'utilisateur des informations sur les points suivants:

— le principe de proportionnalité applicable aux catégories de données collectées, ou auxquelles on a accédé, dans le dispositif;
— les durées de conservation des données;
— les mesures de sécurité mises en œuvre par le responsable du traitement.

Le groupe de travail recommande également que les développeurs d'applications incluent, dans leur politique de confidentialité, des informations destinées à l'utilisateur européen et précisent notamment dans quelle mesure l'application respecte la législation européenne sur la protection des données et, dans le cas d'éventuels transferts de données à caractère personnel de l'Europe vers les Etats-Unis, par exemple, si et dans quelle mesure l'application est conforme au cadre de la «sphère de sécurité».

3.7.2 La forme des informations

La portée essentielle des informations relatives au traitement des données doit être disponible pour l'utilisateur préalablement à l'installation de l'application, par l'intermédiaire du magasin d'applications. Ensuite, les informations pertinentes concernant le traitement des données doivent être également accessibles, après installation, au sein même de l'application.

En tant que coresponsables aux côtés des développeurs d'applications en matière d'informations, les magasins d'applications doivent s'assurer que chaque application fournit les informations essentielles sur le traitement des données à caractère personnel. Ils devraient vérifier les hyperliens vers les pages incluses contenant des informations confidentielles et retirer les applications comportant des liens inopérants ou contenant des informations sur le traitement des données inaccessibles par un autre chemin.

Le groupe de travail recommande que les informations sur le traitement des données à caractère personnel soient également disponibles et facilement localisables, par exemple au sein même du magasin d'applications, et de préférence sur les sites réguliers du développeur d'applications responsable de l'application. Il est inacceptable que l'utilisateur final soit contraint de sonder la toile à la recherche d'informations sur les politiques de traitement des données au lieu d'être informé directement par le développeur d'applications ou tout autre responsable du traitement.

Chaque application devrait, à tout le moins, disposer d'une politique de confidentialité lisible, compréhensible et aisément accessible, contenant toutes les informations décrites ci-dessus. De nombreuses applications ne respectent pas cette exigence de transparence minimale. Selon l'étude de juin 2012 menée par le FPF, 56 % des applications payantes, et près de 30 % des applications gratuites, ne disposent pas d'une politique de confidentialité.

Les applications qui ne traitent pas, ou n'envisagent pas de traiter, des données à caractère personnel, devraient le préciser clairement dans leur politique de confidentialité.

Bien que la quantité d'informations susceptibles d'être présentées sur un petit écran soit naturellement limitée, cette contrainte ne dispense pas de l'obligation d'informer correctement l'utilisateur final. Plusieurs stratégies peuvent être suivies pour garantir la prise de connaissance de la part de l'utilisateur des principaux éléments du service proposé. Le groupe de travail «Article 29» estime que l'utilisation d'avis «stratifiés», tels que détaillés dans son avis 10/2004[43], présente certains avantages. Dans ce système, l'avis de départ présenté à l'utilisateur contient les informations minimales imposées par le cadre juridique de l'Union européenne et des compléments d'information sont disponibles en suivant les liens qui conduisent au texte intégral de la politique de confidentialité. Les informations devraient être présentées directement sur l'écran, de manière à ce qu'elles soient facilement accessibles et parfaitement visibles. Outre les informations complètes adaptées aux petits écrans des dispositifs mobiles dont il a eu connaissance, l'utilisateur doit pouvoir apprendre, en suivant des liens vers des explications plus détaillées contenues par exemple dans la politique de confidentialité, comment l'application utilise ses données à caractère personnel, qui est le responsable du traitement et à quel moment il est en mesure d'exercer ses droits.

Cette approche peut être combinée à l'utilisation d'icônes, d'images, de messages vidéo et audio, et utiliser les notifications contextuelles en temps réel lorsqu'une application accède au carnet d'adresses ou à des photos.[44] Ces icônes doivent être compréhensibles, c.-à-d. claires, explicites et sans ambigüité. Bien évidemment, il est également de la responsabilité du fabricant du système d'exploitation de faciliter l'utilisation de ces icônes.

---

[43] Avis 10/2004 du groupe de travail «Article 29» sur des dispositions davantage harmonisées en matière d'informations (juillet 2004), http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2004/wp100_fr.pdf

[44] Par exemple, l'icône d'avertissement pour le traitement des données de géolocalisation proposée par les iPhones.

En fait, les développeurs d'applications excellent dans la programmation et dans la conception d'interfaces complexes pour petits écrans, et le groupe de travail invite l'industrie à consacrer ce talent créatif à la réalisation de solutions plus innovantes afin d'informer efficacement les utilisateurs sur les dispositifs mobiles. Pour garantir la compréhension réelle des informations par des utilisateurs ne disposant pas de connaissances techniques ou juridiques, le groupe de travail recommande vivement (conformément au rapport du personnel de la FTC) que les stratégies d'information retenues soient testées auprès des consommateurs[45].

3.8 Droits de la personne concernée

Conformément aux articles 12 et 14 de la directive sur la protection des données, les développeurs d'applications et autres responsables du traitement dans l'écosystème des applications mobiles doivent permettre à l'utilisateur d'exercer ses droits d'accès, de rectification, d'effacement et d'opposition au traitement des données. Si un utilisateur exerce son droit d'accès, le responsable du traitement est tenu de fournir les informations relatives aux données en cours de traitement et aux sources de ces données. Si le responsable du traitement prend des décisions automatisées sur la base de données recueillies au préalable, il doit également informer l'utilisateur de la logique qui sous-tend ces décisions. Tel est le cas, par exemple, lorsque la performance ou le comportement des utilisateurs sont évalués, notamment sur la base de données financières ou médicales, ou d'autres données de profil. À la demande de l'utilisateur, le responsable du traitement doit également permettre la rectification, l'effacement ou le verrouillage de données à caractère personnel si celles-ci sont incomplètes, inexactes ou traitées de manière illicite.

Afin que l'utilisateur puisse contrôler le traitement de ses données à caractère personnel, les applications doivent informer ce dernier, de manière claire et visible, de l'existence de ces mécanismes d'accès et de correction. Le groupe de travail «Article 29» recommande la conception et la mise en œuvre d'outils d'accès en ligne simples mais sûrs. Ces outils d'accès devraient de préférence être disponibles dans chaque application, ou accessibles en suivant un lien vers une fonctionnalité en ligne, là où l'utilisateur peut obtenir un accès immédiat à l'ensemble des données en cours de traitement et aux explications nécessaires correspondantes. Des mesures comparables ont été adoptées par des fournisseurs de services en ligne, comme divers tableaux de bord et autres mécanismes d'accès.

Il est particulièrement important de pouvoir obtenir un accès aisé en ligne dans le cas d'applications traitant des profils d'utilisateurs étoffés, comme les applications de réseautage, de socialisation et de messagerie, ou traitant des données sensibles ou financières. Naturellement, l'accès ne devrait être accordé que si l'identité de la personne concernée a été établie, afin d'éviter toute fuite de données vers des tiers. Cependant, cette obligation de vérification de l'identité ne devrait pas entraîner une collecte supplémentaire et excessive de données à caractère personnel relatives à la personne concernée. Dans de nombreux cas, l'authentification pourrait suffire, en lieu et place d'une identification (complète).

En outre, l'utilisateur devrait toujours avoir la possibilité de retirer son consentement de manière simple et peu fastidieuse. La personne concernée peut retirer son consentement au traitement des données de plusieurs façons différentes et pour divers motifs. L'option

[45] Rapport du personnel de la FTC, note 6 supra, p. 16.

autorisant le retrait du consentement devrait de préférence être offerte par le biais des mécanismes facilement accessibles mentionnés ci-dessus. Il doit être possible de désinstaller des applications et, dès lors, de retirer toutes les données à caractère personnel, même sur les serveurs du/des responsable(s) du traitement. Afin de permettre à l'utilisateur de demander au développeur de l'application la suppression de ses données, il est important que le fabricant du système d'exploitation transmette au développeur de l'application un signal lorsqu'un utilisateur désinstalle l'application. Ce signal pourrait être transmis par l'API. En principe, après la désinstallation de l'application par l'utilisateur, le développeur ne bénéficie plus d'un fondement juridique l'autorisant à poursuivre le traitement des données à caractère personnel relatives à cet utilisateur, et doit donc supprimer toutes les données. Un développeur d'applications souhaitant conserver certaines données, par exemple afin de faciliter la réinstallation de l'application, doit introduire une requête de consentement séparée au cours du processus de désinstallation, en demandant à l'utilisateur d'autoriser une durée de conservation supplémentaire bien définie. L'unique exception à cette règle est l'existence éventuelle d'obligations juridiques imposant la conservation de certaines données à des fins particulières, par exemple des obligations d'ordre fiscal dans le cas de transactions financières.[46]

3.9 Durées de conservation

Les développeurs d'applications doivent tenir compte de la conservation des données collectées par le biais de l'application et des risques que celle-ci entraîne en matière de protection des données. Les durées de conservation spécifiques dépendront de la finalité de l'application et de l'importance des données pour l'utilisateur final. Par exemple, dans le cas d'une application permettant le partage de calendriers, d'agendas ou de photos, la durée de conservation est contrôlée par l'utilisateur final alors que pour une application de navigation, le stockage des 10 dernières localisations récemment visitées pourrait suffire. Les développeurs d'applications devraient également tenir compte des données des utilisateurs qui n'ont pas eu recours à l'application depuis longtemps. Il se peut que ces utilisateurs aient perdu leur dispositif mobile ou changé de dispositif sans désinstaller activement toutes les applications dans le dispositif d'origine. Les développeurs d'applications devraient dès lors prédéfinir un délai d'inactivité au terme duquel le compte serait considéré comme ayant expiré, et veiller à ce que l'utilisateur soit informé de ce délai. Au terme de ce délai, le responsable du traitement devrait avertir l'utilisateur et lui donner la possibilité de récupérer les données à caractère personnel. Si l'utilisateur ne réagit pas à cet avertissement, les données à caractère personnel le concernant et relatives à l'utilisation de l'application devraient être anonymisées de manière irréversible, ou supprimées. Le délai de rappel dépend de la finalité de l'application et du lieu de stockage des données. S'il agit de données stockées dans le dispositif même, comme le score élevé d'un jeu, les données peuvent être conservées aussi longtemps que l'application reste installée. S'il s'agit de données utilisées uniquement

[46] Le groupe de travail rappelle que l'obligation de conservation des données imposée par l'Europe (directive 2006/24/CE) ne s'applique pas à l'ensemble des services de la société de l'information, parmi lesquels les applications, et qu'elle ne peut donc être invoquée comme fondement juridique pour poursuivre le traitement des données concernant l'utilisateur d'une application une fois que ce dernier a supprimé l'application. Le groupe de travail saisit cette occasion pour souligner le caractère particulièrement risqué des données relatives au trafic, qui exigent des précautions particulières et des garanties spécifiques au trafic «en soi» – comme souligné dans le rapport du groupe de travail «Article 29» sur le respect de la directive relative à la conservation des données (WP172) – et pour lesquelles toutes les parties concernées ont été invitées à mettre en œuvre les mesures de sécurité appropriées.

une fois par an, comme des informations sur une station de ski par exemple, le délai de rappel pourrait être de 15 mois.

3.10 Les enfants

Les enfants sont des utilisateurs assidus d'applications, qu'il s'agisse de leur dispositif propre ou de dispositifs partagés (par exemple, l'appareil des parents, des frères et sœurs, ou celui d'un établissement scolaire). Le marché des applications ciblant les enfants est donc naturellement vaste et diversifié. Par ailleurs, cependant, les enfants ne comprennent/connaissent pas ou comprennent/connaissent peu la portée et la sensibilité des données auxquelles les applications sont susceptibles d'accéder, ni l'importance du partage de données avec des tiers à des fins publicitaires.

Le groupe de travail a traité en profondeur la question du traitement des données des enfants dans son avis 2/2009 sur la protection des données à caractère personnel de l'enfant et n'aborde dans ce point qu'un certain nombre de risques et de recommandations plus spécifiques aux applications.[47]

Les développeurs d'applications et autres responsables du traitement devraient prendre en considération l'âge limite définissant le statut d'enfant ou de mineur dans les législations nationales, lorsque l'autorisation parentale pour le traitement des données est une condition préalable au traitement licite des données par les applications[48].

Lorsque le consentement d'un mineur peut être légalement obtenu et que l'application est destinée à l'utilisation par un enfant ou un mineur, le responsable du traitement doit être attentif au fait que le mineur peut avoir une compréhension limitée du traitement des données et qu'il n'accorde que peu d'attention aux informations sur le sujet. En raison de la vulnérabilité générale d'un enfant et compte tenu du fait que les données à caractère personnel doivent être traitées de manière loyale et licite, les responsables d'un traitement ciblant les enfants devraient respecter de façon encore plus stricte les principes de minimisation des données et de limitation de la finalité. Plus particulièrement, les responsables du traitement ne devraient pas utiliser les données de l'enfant à des fins de publicité comportementale, que ce soit directement ou indirectement, dans la mesure où une telle pratique n'entre pas dans la sphère de compréhension d'un enfant et dépasse dès lors les limites d'un traitement loyal.

Le groupe de travail partage les préoccupations exprimées par la Federal Trade Commission dans son rapport sur les applications mobiles destinées aux enfants[49].

Les développeurs d'applications, en collaboration avec les magasins d'applications et les fabricants de systèmes d'exploitation et de dispositifs, devraient présenter les informations

---

[47] WP 160, avis 2/2009 sur la protection des données à caractère personnel de l'enfant (Principes généraux et cas particulier des écoles) (11 février 2009), http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp160_fr.pdf

[48] Dans les États membres de l'Union européenne, cet âge varie de 12 à 18 ans.

[49] Rapport du personnel de la FTC «Mobile Apps for Kids: Current Privacy Disclosures are Disappointing» (février 2012), http://www.ftc.gov/os/2012/02/120216mobile_apps_kids.pdf. «*Alors qu'il a relevé un large éventail d'applications pour enfants créées par des centaines de développeurs différents, le personnel a trouvé peu, ou pas, d'informations sur le marché des applications en rapport avec la collecte de données et les pratiques de partage de ces applications.*»

utiles de manière simple, dans un langage adapté à un jeune âge. Les responsables du traitement devraient également s'abstenir plus spécifiquement de collecter des données relatives aux parents ou aux membres de la famille de l'enfant, telles que des informations financières ou des catégories particulières d'information comme des données médicales.

4 Conclusions et recommandations

Bon nombre des différents types de données disponibles dans un dispositif mobile intelligent sont des données à caractère personnel. Le cadre juridique de référence est la directive sur la protection des données, complétée par la disposition spécifique relative au consentement contenue à l'article 5, paragraphe 3, de la directive «vie privée et communications électroniques». Ces règles concernent toute application destinée aux utilisateurs au sein de l'Union européenne, indépendamment de l'endroit où est établi le développeur ou le magasin d'applications.

Le caractère fragmenté de l'écosystème applicatif, le large éventail de possibilités techniques permettant l'accès aux données stockées dans des dispositifs mobiles ou générées par ces derniers, ainsi que le manque de connaissances juridiques de la part des développeurs entraînent un certain nombre de risques sérieux en matière de protection des données pour les utilisateurs d'applications. Ces risques découlent aussi bien d'un manque de transparence et de connaissance de la part l'utilisateur que des mesures de sécurité insuffisantes, des mécanismes de consentement non valables, d'une tendance à la maximisation des données et de finalités de traitement trop dispersées.

En matière de protection des données, les responsabilités se chevauchent entre les différentes parties associées au développement, à la distribution et aux performances techniques des applications. La plupart des conclusions et des recommandations s'adressent aux développeurs d'applications (dans la mesure où ces derniers contrôlent en grande partie la manière précise dont le traitement est effectué ou dont les informations sont présentées dans l'application). Souvent, cependant, pour respecter les normes les plus élevées en matière de protection des données et de la vie privée, les développeurs doivent collaborer avec d'autres parties de l'écosystème applicatif, telles que les fabricants de systèmes d'exploitation et de dispositifs, les magasins d'applications et les tiers (fournisseurs de solutions analytiques ou réseaux publicitaires, par exemple).

Les développeurs d'applications doivent:

- connaître et respecter leurs obligations en tant que responsables du traitement dès lors qu'ils traitent des données en provenance et à propos d'utilisateurs;
- connaître et respecter leurs obligations en tant que responsables du traitement dès lors qu'ils collaborent avec des sous-traitants, notamment dans le cadre de l'externalisation de la collecte et du traitement de données à caractère personnel auprès de développeurs, de programmeurs ou de fournisseurs de services de stockage sur le nuage, par exemple;
- demander le consentement avant le début de la récupération ou du placement de données sur le dispositif, c.-à-d. préalablement à l'installation de l'application. Ce consentement doit être libre, spécifique et informé;
- demander un consentement détaillé pour chaque type de données auxquelles l'application aura accès, du moins pour les catégories: localisation, contacts, identifiant unique du dispositif, identité de la personne concernée, identité du téléphone, données relatives aux cartes de crédit et aux paiements, téléphonie et SMS, historique de navigation, courriels, éléments d'identification pour les réseaux sociaux et biométrie;

- être conscients du fait que le consentement n'autorise pas un traitement de données excessif ou disproportionné;
- communiquer les finalités du traitement des données de manière bien définie et compréhensible, préalablement à l'installation de l'application, et ne pas modifier ces finalités sans un renouvellement du consentement; fournir des informations complètes en cas d'utilisation par des tiers, notamment à des fins publicitaires ou analytiques;
- permettre aux utilisateurs de révoquer leur consentement, de désinstaller l'application et de supprimer les données selon les besoins;
- respecter le principe de minimisation des données et ne collecter que les données strictement nécessaires à la réalisation de la fonctionnalité souhaitée;
- prendre les mesures techniques et d'organisation nécessaires afin de garantir la protection des données à caractère personnel objet du traitement, à tous les stades de la conception et de la mise en place de l'application (principe de la vie privée dès la conception), tel que défini au point 3.6 du présent avis;
- fournir un point de contact unique pour les utilisateurs de l'application;
- proposer une politique de confidentialité lisible, compréhensible et aisément accessible, qui fournisse à l'utilisateur au moins les informations suivantes:
  - leur identité et leurs coordonnées,
  - les catégories précises de données à caractère personnel que l'application envisage de collecter et de traiter,
  - la finalité du traitement des données (les objectifs précis),
  - la notification éventuelle que les données seront transmises à des tiers (pas uniquement une description générale mais une information détaillée sur les destinataires des données),
  - les droits dont bénéficient l'utilisateur, concernant le retrait du consentement et la suppression de données;
- permettre à l'utilisateur d'exercer ses droits d'accès, de rectification, d'effacement et d'opposition au traitement des données, et l'informer de l'existence de ces mécanismes;
- fixer une durée de conservation raisonnable pour les données collectées par le biais de l'application et prédéfinir un délai d'inactivité au terme duquel le compte sera considéré comme ayant expiré;
- en ce qui concerne les applications destinées aux enfants: tenir compte de l'âge limite définissant le statut d'enfant ou de mineur dans les législations nationales, choisir l'approche la plus restrictive pour le traitement des données, dans le respect total des principes de minimisation des données et de limitation de la finalité, s'abstenir de traiter les données de l'enfant à des fins de publicité comportementale, directement ou indirectement, et s'abstenir de collecter des données par l'intermédiaire de l'enfant sur sa famille et/ou ses amis.

Le groupe de travail recommande que les développeurs d'application:

- prennent connaissance des lignes directrices pertinentes concernant les risques et les mesures de sécurité;
- informent l'utilisateur de manière proactive de toute violation des données à caractère personnel conformément aux exigences de la directive «vie privée et communications électroniques»;
- informent l'utilisateur du principe de proportionnalité applicable aux types de données collectées dans le dispositif, ou auxquelles on a accédé, des durées de conservation des données et des mesures de sécurité mises en œuvre;

- élaborent des outils permettant à l'utilisateur de personnaliser les durées de conservation de ses données à caractère personnel en fonction de préférences et de contextes spécifiques, et ne proposent pas des durées de conservation prédéfinies;
- incluent dans leur politique de confidentialité des informations destinées aux utilisateurs européens;
- élaborent et mettent en place des outils d'accès simples mais sûrs à l'intention de l'utilisateur, sans collecter des données à caractère personnel supplémentaires et excessives;
- en collaboration avec les fabricants de systèmes d'exploitation et de dispositifs, ainsi qu'avec les magasins d'applications, utilisent leur talent de créativité pour élaborer des solutions innovantes de manière à informer correctement l'utilisateur sur le dispositif mobile, par exemple à l'aide d'avis d'information stratifiés complétés par des icônes explicites.

Les magasins d'applications doivent:

- connaître et respecter leurs obligations en tant que responsables du traitement dès lors qu'ils traitent des données en provenance et à propos d'utilisateurs;
- garantir le respect des obligations par le développeur d'applications en matière d'information, en ce qui concerne notamment les types de données auxquelles l'application peut accéder, les finalités envisagées et la notification éventuelle selon laquelle les données sont partagées avec des tiers;
- accorder une attention particulière aux applications destinées aux enfants afin de prémunir ces derniers contre tout traitement illicite de leurs données, et veiller plus précisément à ce que les informations utiles soient présentées de manière simple, dans un langage adapté à un jeune âge;
- fournir des informations détaillées sur les contrôles réellement effectués lors de la proposition des applications par les développeurs, y compris sur les vérifications visant à évaluer les mesures de protection des données et de la vie privée.

Le groupe de travail recommande que les magasins d'applications:

- en collaboration avec le fabricant du système d'exploitation, élaborent des outils de contrôle à l'intention de l'utilisateur, tels que des symboles représentant l'accès aux données présentes dans le dispositif mobile ou générées par celui-ci;
- soumettent toutes les applications à un mécanisme de réputation publique;
- instaurent un mécanisme de désinstallation à distance respectueux de la vie privée;
- proposent des canaux de communication pour le retour d'informations des utilisateurs sur les questions touchant la vie privée et/ou la sécurité;
- collaborent avec les développeurs d'applications afin d'informer de manière proactive l'utilisateur de toute violation des données à caractère personnel;
- attirent l'attention des développeurs d'applications sur les spécificités de la législation européenne préalablement à la proposition d'applications en Europe, notamment en ce qui concerne l'exigence de consentement et le transfert de données à caractère personnel vers des pays non membres de l'Union européenne.

Les fabricants de systèmes d'exploitation et de dispositifs doivent:

- mettre à jour les API, les règles de stockage et les interfaces des utilisateurs afin que ces derniers aient un contrôle suffisant leur permettant de donner un consentement valable en vue du traitement des données par les applications;

- mettre en place des mécanismes de requête du consentement dans les systèmes d'exploitation lors du premier lancement de l'application ou lorsque l'application tente d'accéder pour la première fois à l'une des catégories de données dont l'incidence sur la vie privée est importante;
- appliquer les principes de «protection de la vie privée dès la conception» afin de prévenir tout contrôle caché de l'utilisateur;
- garantir la sécurité du traitement;
- veiller à ce que les (paramètres par défaut des) applications préinstallées soient conformes à la législation européenne sur la protection des données;
- proposer un accès détaillé aux données, capteurs et services, de sorte que le développeur d'applications ne puisse accéder qu'aux données nécessaires à son application;
- fournir des solutions conviviales et efficaces contre le traçage des annonceurs et de toute autre partie tierce. Les paramètres par défaut doivent être définis de manière à éviter tout traçage;
- garantir la disponibilité de mécanismes adéquats permettant d'informer et de sensibiliser l'utilisateur final sur les actions éventuelles des applications et sur le type de données auxquelles elles peuvent accéder;
- veiller à ce que tout accès à une catégorie de données se reflète dans les informations fournies à l'utilisateur préalablement à l'installation de l'application: les catégories présentées doivent être claires et compréhensibles;
- instaurer un environnement privilégiant la sécurité, avec des outils empêchant la diffusion d'applications malveillantes et permettant l'installation et la désinstallation aisée de chaque fonctionnalité.

Le groupe de travail recommande que les fabricants de systèmes d'exploitation et de dispositifs:

- permettent à l'utilisateur de désinstaller les applications et transmettent un signal (éventuellement par le biais de l'API) au développeur d'applications en vue de la suppression des données pertinentes de l'utilisateur;
- proposent et fournissent systématiquement des mises à jour de sécurité régulières;
- veillent à ce que les méthodes et les fonctions permettant l'accès aux données à caractère personnel comportent des fonctionnalités en vue de l'introduction de demandes de consentement détaillé;
- contribuent activement à l'élaboration et à la mise en place d'icônes alertant l'utilisateur des différents usages que les applications font des données;
- élaborent dans les dispositifs des pistes d'audit claires de sorte que l'utilisateur final puisse repérer clairement les applications accédant aux données présentes dans son dispositif et puisse comparer le volume de trafic sortant par application au trafic généré par lui-même.

Les tiers doivent:

- connaître et respecter leurs obligations en tant que responsables du traitement dès lors qu'ils traitent des données à propos des utilisateurs;
- respectent l'obligation de consentement visée à l'article 5, paragraphe 3, de la directive «vie privée et communications électroniques» lors de la lecture ou de l'écriture de données dans les dispositifs mobiles, en collaboration avec les développeurs et/ou les magasins d'applications, qui fournissent essentiellement à l'utilisateur des informations sur les finalités du traitement des données;

- s’abstenir de contourner tout mécanisme conçu pour prévenir le traçage, comme c’est actuellement souvent le cas avec les fonctionnalités «ne pas suivre» embarquées au sein des navigateurs;
- lorsqu’ils représentent des fournisseurs de services de communications et distribuent des appareils siglés, garantir le consentement valable des utilisateurs pour les applications préinstallées et assumer leurs justes responsabilités lorsqu’ils contribuent à définir certaines caractéristiques du dispositif et du système d’exploitation, notamment lorsqu’ils limitent l’accès de l’utilisateur à certains paramètres de configuration ou qu’ils filtrent les correctifs (fonctionnels et de sécurité) fournis par le fabricant du dispositif ou du système d’exploitation;
- en tant qu’annonceurs, éviter plus particulièrement de proposer des publicités sortant du contexte de l’application. Des exemples d’une telle pratique sont l’insertion d’annonces à la suite d’une modification des paramètres de navigation ou le placement d’icônes sur le bureau mobile. Ils doivent s’abstenir d’utiliser les identifiants uniques du dispositif ou de l’abonné à des fins de traçage;
- s’abstenir de traiter les données des enfants à des fins de publicité comportementale, directement ou indirectement. Ils doivent également appliquer des mesures de sécurité appropriées, telles que la transmission sécurisée et le stockage encrypté des identifiants uniques du dispositif et de l’utilisateur, et d’autres données à caractère personnel.

Le groupe de travail recommande que les tiers:

- élaborent et mettent en ligne des outils d’accès simples mais sûrs à l’intention des utilisateurs, en évitant de collecter des données à caractère personnel supplémentaires et excessives;
- collectent et traitent exclusivement des données qui soient pertinentes pour le contexte dans lequel l’utilisateur fournit ces données.