

Le G29 publie ses recommandations sur l'utilisation de données personnelles via les applications mobiles

[DONNEES PERSONNELLES]

Avis du G29 02/2013 sur les applications destinées aux dispositifs intelligents, adopté le 27 février 2013

Le développement constant des applications disponibles sur les smartphones, tablettes et autres appareils mobiles conjugué à leur succès croissant auprès du public ont conduit le G29 à rappeler les règles juridiques applicables aux différents acteurs de ce nouvel écosystème en matière de protection des données personnelles et à émettre des recommandations pratiques pour leur mise en œuvre.

Selon les chiffres de Médiamétrie, 24 millions de français disposeraient aujourd'hui de téléphones mobiles intelligents dits Smartphones. Ces appareils mobiles proposent des applications logicielles de plus en plus performantes dont le fonctionnement s'appuie sur une quantité importante d'informations qu'il s'agisse de données personnelles stockées par l'utilisateur dans l'appareil ou de données enregistrées par l'appareil lui-même.

Le G29 rappelle que la législation européenne propre à la protection des données personnelles s'applique dès lors que les applications sont destinées aux utilisateurs résidant au sein de l'Union Européenne, quel que soit le pays où sont établis les divers intervenants participant à la collecte et au traitement de leurs données.

Plusieurs intervenants techniques ou économiques participent en effet au développement, à la distribution et l'exploitation des applications à savoir les développeurs, les magasins de mise à disposition, les éditeurs de système d'exploitation, les fabricants de dispositifs ainsi que les régies publicitaires ou les annonceurs.

Si la responsabilité en matière de protection des données peut être partagée entre ces différents acteurs, le G29 considère que les développeurs et les magasins d'application gardent un rôle clef dans la gestion des données personnelles des utilisateurs, dans la mesure où ils contrôlent en grande partie les modalités de mise en œuvre du traitement ou de présentation des informations présentées dans l'application. C'est la raison pour laquelle le G29 estime que le respect des obligations prévues par la législation pèse essentiellement sur ces derniers.

Les données personnelles traitées par les applications couvrent des catégories variées telles que les données de localisation, les contacts, les identifiants uniques des appareils, l'identité de l'utilisateur, les coordonnées bancaires, les journaux d'appels, l'historique de navigation, les photos ou vidéos ainsi que les données d'authentification, dont l'incidence sur la vie privée de l'utilisateur peut être significative.

Aussi, le groupe européen rappelle que les fabricants de dispositifs, les développeurs et les magasins d'applications doivent intégrer la protection des données dès le début de la conception des outils ou services d'applications comprenant « *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* ».

Parmi les principales règles applicables au traitement des données via les applications, le G29 met particulièrement l'accent sur l'obligation relative à l'obtention du consentement préalable de l'utilisateur dont le fondement juridique est double:

- (i) D'une part, en vertu de l'article 5 §3 de la directive «*vie privée et communication électronique*», le consentement *préalable* de l'utilisateur est requis pour permettre à l'application d'installer des informations dans le système de l'appareil et d'accéder à d'autres informations stockées dans le dispositif (contacts, photos, vidéos et autres documents), et ce indépendamment du caractère personnel ou non des données concernées (cette disposition vise en particulier la pose de cookies) ;
- (ii) D'autre part, conformément à la directive 95/46/CE sur la protection des personnes physiques à l'égard du traitement de leurs données personnelles, le consentement de l'utilisateur est également nécessaire pour autoriser le traitement de différents types de données à caractère personnel le concernant.

Ces deux dispositions imposant l'obtention du consentement sont par conséquent simultanément applicables et les modalités de leur recueil peuvent mises en œuvre de façon concomitante au cours de l'installation de l'application ou lors de la collecte des données personnelles, dès lors qu'une information claire et sans ambiguïté est communiquée à l'utilisateur sur la portée et les finalités de son accord. Il est néanmoins rappelé que l'utilisateur doit garder la possibilité de retirer son consentement de manière simple et efficace.

Le G29 souligne ensuite l'obligation pour les développeurs d'application de respecter les principes de «*limitation de finalité et de minimisation des données*» en définissant de façon scrupuleuse les données qui sont strictement nécessaires à la réalisation de la fonctionnalité de l'application et en excluant toute modification inopinée des conditions d'utilisation du traitement mis en œuvre.

Aussi, les traitements mis en œuvre via les applications ne devraient pas donner lieu à une identification permanente et un traçage continu des utilisateurs mais au contraire privilégier des identifiants temporaires ou ciblant une application. De même, s'agissant de la conservation des données, il est recommandé aux développeurs de prédéfinir un délai d'inactivité au terme duquel le compte serait considéré comme ayant expiré et veiller à ce que l'utilisateur en soit informé.

Pour rendre effectif le respect de ces différents principes, le G29 met en exergue l'exigence de transparence et de disponibilité de l'information qui doit être fournie aux utilisateurs. Il considère à ce titre que «*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*».

Aussi les contraintes de format liées au petit écran des appareils mobiles ne dispensent pas les développeurs d'application d'informer correctement l'utilisateur final des modalités du traitement de ses données, notamment via la communication stratifiée d'informations conduisant l'utilisateur à accéder à des informations plus détaillées en suivant différents liens. Cette approche peut être combinée à l'utilisation d'icônes ou messages vidéo et audio.

Selon ce schéma, le G29 indique que deux niveaux d'information peuvent être successivement communiqués :

- (i) Le premier niveau porte sur les informations essentielles à l'obtention du consentement qui doivent être fournies avant l'installation de l'application. Ces informations portent sur l'identité du responsable, les catégories précises de données collectées par le développeur, la finalité du traitement, la confirmation de la transmission des données à des tiers ainsi que la manière dont l'utilisateur peut retirer son consentement ou supprimer ses données ;
- (ii) Le second niveau porte sur les informations concourant au traitement loyal des données qui peuvent être fournies dans la politique de confidentialité des développeurs. Ces informations portent sur le principe de proportionnalité applicable aux données collectées, les durées de conservation et les mesures de sécurité utilisées par le responsable du traitement.

Le G29 précise également que les magasins d'application doivent jouer un rôle essentiel dans la communication de ces informations en s'assurant que chaque application utilise des liens hypertextes valides renvoyant vers les pages d'informations adéquates. A défaut, ces applications devraient être retirées de leurs plateformes.

L'ensemble des recommandations du G29 sous-tendent un objectif de transparence et de contrôle des données par les utilisateurs eux-mêmes qui sont les principaux garants de la protection de leur propre vie privée. A cet égard, l'évaluation par le public des outils de sécurité et de confidentialité mis en œuvre par les applications est encouragée par le G29 pour instaurer un mécanisme de réputation contribuant à instaurer un climat de confiance mutuelle entre les différents acteurs.

Sabine DELOGES