

Applications mobiles : la CNIL présente son plan d'action pour protéger votre vie privée

24 novembre 2022

Les applications mobiles sont un des principaux moyens d'accès à des contenus et des services numériques. La CNIL a établi un plan d'action pour les années à venir afin d'accompagner leur mise en conformité et de protéger la vie privée des utilisateurs.

Le contexte

Au quatrième trimestre 2021, les Français ont utilisé des applications mobiles durant 170 millions d'heures, **soit presque le double du temps passé au premier trimestre 2018** (source : « State of Mobile 2022 », App Annie). Cette forte augmentation révèle une rapide évolution des usages, le smartphone devient un peu plus chaque jour **le premier vecteur d'accès au numérique**.

L'offre d'applications mobiles est elle aussi croissante et implique de nombreux acteurs : les développeurs de l'application, les fournisseurs de systèmes d'exploitation, les gestionnaires de magasins d'applications, les éditeurs de kit de développement logiciels (*software development kits* ou SDK) liés à des réseaux sociaux ou à des fonctionnalités techniques, etc. En pratique, des transferts de données ont souvent lieu entre ces différents acteurs, avec des partages de responsabilité parfois mal définis. **Si les principes et obligations en matière de protection des données sont désormais bien connus des opérateurs de sites web et font l'objet de recommandations de la part de la CNIL, leur mise en œuvre dans le contexte des applications mobiles peut encore être clarifiée.**

Côté utilisateurs, **le smartphone, terminal personnel par définition, relève de la sphère privée et intime**. Il est essentiel pour chacun de pouvoir contrôler les données auxquelles les applications mobiles ont accès. Pour autant à l'heure actuelle, **les traitements de données peuvent être opaques**. En particulier, les informations sur l'existence de collectes de données et les raisons pour lesquelles celles-ci sont collectées sont souvent peu claires. De même, l'utilisateur peut avoir des difficultés à comprendre la nature des autorisations qui lui sont demandées, ce qui complique l'expression de ses choix. Enfin, les smartphones embarquent de nombreux capteurs plus ou moins connus des utilisateurs (caméra, GPS, base de contacts, accéléromètre, etc.) et qui peuvent permettre aux applications d'accéder à des données dont la collecte peut se révéler très intrusive.

Compte tenu des enjeux importants de protection de la vie privée liés à l'usage de smartphone, **la CNIL a décidé d'agir de manière prioritaire sur ces sujets**.

Les axes de travail

La CNIL entend suivre un plan d'action en trois étapes. **Tout d'abord**, la CNIL va poursuivre ses travaux pour avoir une complète maîtrise du sujet, notamment technique. **Ensuite**, elle mettra à profit les connaissances acquises pour accompagner les professionnels et informer les citoyens, par exemple sous la forme de guides et de recommandations. **Enfin**, elle procédera à des contrôles ciblés et, si besoin, elle engagera des **actions répressives** vis-à-vis des organismes ne respectant pas leurs obligations.

Etape 1 : une veille et un dialogue pour mieux comprendre le secteur

Afin d'identifier les leviers d'action les plus efficaces pour améliorer la protection de la vie privée, la CNIL a organisé, au cours des mois de septembre et d'octobre, une **série de rencontres avec différents acteurs représentatifs de l'écosystème** (fournisseurs de systèmes d'exploitation, développeurs d'applications, fournisseurs de SDK, etc. mais aussi acteurs de la société civile et de la recherche étudiant les pratiques de l'écosystème mobile).

Cette démarche doit **permettre à la CNIL de s'assurer d'une bonne compréhension du secteur**. Elle complète ainsi les travaux déjà menés : à titre d'exemple, la question des applications mobiles a été abordée lors du [Privacy Research Day](#) que la CNIL a organisé le 28 juin dernier. Le [Prix CNIL-Inria](#) attribué en 2021 portait également sur ce sujet.

Le LINC, le Laboratoire d'innovation numérique de la CNIL, a également engagé des travaux sur certaines données particulièrement « sensibles » (même si elles ne le sont pas nécessairement [au sens du RGPD](#)), notamment [avec une étude sur les données de géolocalisation obtenues via des applications mobiles](#), permettant de mieux comprendre les risques associés à la collecte de ce type de données.

Etape 2 : un accompagnement et une communication dédiés

Sur la base de ces travaux, la CNIL publiera des recommandations sur le sujet des applications mobiles pour que chaque acteur ait une bonne compréhension de ses obligations et pour faciliter leur mise en conformité.

Des outils pratiques (fiche ou guide pratique, checklist d'auto-évaluation, etc.) **à destination des utilisateurs pourront également être publiés pour les sensibiliser aux risques et impacts réels que représente le traitement de leurs données au travers des applications mobiles**. En particulier, les problématiques liées aux applications s'adressant à des publics vulnérables ou traitant des données sensibles (applications médicales ou destinées aux enfants, femmes enceintes, etc.) ou aux collectes de données provenant des capteurs des smartphones feront l'objet de travaux spécifiques.

Etape 3 : des contrôles et des sanctions à la mesure des enjeux

En fonction des observations de terrain effectuées à l’occasion des travaux menés pour clarifier le cadre légal, la CNIL pourra décider de **mettre en œuvre un plan de contrôle de grande ampleur**, comme cela avait été réalisé dans le cadre des actions liés aux cookies et autres traceurs. Elle pourrait en particulier se concentrer sur les traitements susceptibles d’engendrer des risques spécifiques importants pour les personnes, par exemple parce qu’ils ciblent des publics vulnérables ou qu’ils collectent des données de manière particulièrement intrusive.

Ces actions viendraient compléter les contrôles déjà régulièrement menés sur la base de plaintes et visant à s'assurer du respect des principes fondamentaux du RGPD par les éditeurs d’applications mobiles.

À l’issue de ces contrôles, en fonction de la nature et de l’ampleur des manquements éventuellement constatés, **la CNIL sera susceptible de prendre des mesures correctrices, notamment des sanctions pécuniaires.**

La mise en œuvre des différentes étapes précitées permet à la CNIL de procéder à une régulation équilibrée qui prend en compte les réalités opérationnelles, économiques et techniques d’un secteur, tout en assurant une protection effective des droits et libertés des utilisateurs.