Consultation publique sur le projet de recommandation relative aux applications mobiles

Synthèse des contributions et réponses de la CNIL

Septembre 2024

Du 21 juillet au 8 octobre 2023, la CNIL a lancé une consultation publique sur son projet de recommandation relative aux applications mobiles. Les contributions reçues ont alimenté les travaux de la CNIL et lui ont permis d'adopter la version définitive de la recommandation.

Cette synthèse présente les observations les plus importantes, ainsi que les éléments de réponse de la CNIL.

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

Les participants à la consultation

Le projet de recommandation a reçu les contributions de **18 acteurs lors de la consultation publique** :

- 3 associations professionnelles ;
- 2 fournisseurs de systèmes d'exploitation (OS) ;
- 3 fournisseurs de kits de développement logiciel (SDK) ;
- 6 éditeurs d'applications ;
- 1 cabinet de conseil en protection des données personnelles ;
- 3 personnes privées.

Ces contributions ont permis à la CNIL :

- de vérifier son caractère opérationnel au regard des contraintes, notamment techniques, auxquelles les acteurs sont soumis ;
- de faire évoluer son projet afin de prendre en compte les préoccupations les plus fréquemment partagées par les contributeurs ;
- de clarifier, sur la forme comme sur le fond, sa recommandation sur plusieurs points : la CNIL a notamment mieux distingué ce qui relève de l'obligation, de la recommandation ou de la bonne pratique. Elle a explicité les interactions entre ses recommandations et la prise en compte des enjeux concurrentiels, et recentré ses recommandations relatives aux systèmes de permissions.

Sur le formalisme de la recommandation

Synthèse des contributions

Les contributions ont révélé un besoin de clarifier **la portée juridique des dispositions présentes dans la recommandation** afin, en particulier, qu'il soit facile d'identifier les dispositions qui relèvent d'une obligation légale.

Certains répondants ont jugé que la **lisibilité du document pouvait être améliorée**, en raison de sa longueur et de sa volonté d'exhaustivité. La segmentation par acteurs a notamment été critiquée, certaines parties pouvant comprendre des renvois voire des redondances.

Éléments de réponse de la CNIL

Afin de fournir de la sécurité juridique aux acteurs de l'écosystème, la CNIL a fait évoluer **la forme de la recommandation afin de clarifier la portée juridique de chacune des dispositions du document**. La nouvelle rédaction a été conçue afin qu'il soit aisé de distinguer, dès la première lecture :

- les dispositions revêtant une portée obligatoire et réglementaire ;
- les recommandations qui proposent un moyen pratique (parmi d'autres) de se conformer à la règle de droit ;
- les bonnes pratiques qui ne sont pas imposées par les textes mais permettent de renforcer la protection des droits et des données personnelles des utilisateurs.

Par ailleurs, la segmentation par catégories d'acteurs a été maintenue pour permettre à chacun, notamment ceux dont les ressources juridiques ou techniques sont limitées, **d'identifier facilement l'ensemble des éléments qui les concernent,** tout en ayant accès **une vision d'ensemble de l'écosystème**.

La CNIL **accompagnera les acteurs professionnels** ces prochains mois, notamment à travers des webinaires, afin d'aider **les acteurs à se saisir de la recommandation**.

Sur la compatibilité des recommandations avec d'autres textes et le droit de la concurrence en général

Synthèse des contributions

Certains répondants ont soulevé des **problématiques liées à l'articulation entre le projet de recommandation et le droit de la concurrence sur un marché déjà caractérisé par un fort déséquilibre concurrentiel.** Leurs inquiétudes étaient :

- que les recommandations de la CNIL soient de nature à renforcer la position dominante de certains acteurs majeurs présents à plusieurs niveaux la chaîne de valeur des applications mobiles, par exemple en conduisant à des collectes de données supplémentaires par ces acteurs ou en leur donnant la possibilité de priver les tiers de l'accès à certaines données ;
- que ces acteurs se soustraient à certaines des recommandations de la CNIL, celles-ci étant construites par typologie d'acteur.

Certains contributeurs se sont en outre inquiétés du coût de la mise en conformité que pourrait induire la recommandation de la CNIL, notamment pour les acteurs les plus fragiles économiquement.

Éléments de réponse de la CNIL

La recommandation finale de la CNIL tient compte des enjeux posés par le droit de la concurrence et le règlement sur les marchés numériques (*Digital Markets Act* ou DMA), éclairés par l'avis de l'Autorité de la concurrence et les diverses contributions des acteurs de l'écosystème. Elle rappelle notamment :

- **que la recommandation s'applique dans le respect du droit de la concurrence** et du DMA. Par exemple, la recommandation souligne que les données générées par les entreprises dans le cadre de leur utilisation des services de plateforme essentiels visés dans le DMA (contrôleurs d'accès) ne doivent pas être utilisées par ces derniers en concurrence avec ces entreprises.

- que **tout éditeur d'application mettant en œuvre un traitement de données personnelles est soumis aux mêmes règles en matière de protection des données personnelles,** ce qui inclut de fait les acteurs majeurs présents à plusieurs niveaux de la chaîne de valeur des applications mobiles.

Concernant les coûts de mise en conformité, la CNIL a adopté une approche équilibrée et pragmatique pour faire en sorte que toutes les entreprises aient des exigences de conformité compatibles avec leur taille.

La CNIL a veillé à ce que sa recommandation soit compatible avec une concurrence saine et une innovation respectueuse de la vie privée. La recommandation ne crée aucune règle nouvelle et a, à l'inverse, comme objectif de **faciliter la mise en conformité avec la loi des acteurs qui ne disposent pas nécessairement des ressources internes pour apprécier correctement la répartition des obligations et encadrer les relations avec leurs partenaires commerciaux**.

Sur les qualifications et responsabilités des acteurs de l'écosystème mobile

Synthèse des contributions

Les développements relatifs à la qualification des acteurs ont fait l'objet de plusieurs remarques (partie 4 de la recommandation) :

- des critiques ont été formulées concernant les exemples proposés, considérés comme trop détaillés et prescriptifs par certains contributeurs ; peu clairs ou trop généraux par d'autres ;
- les cas de responsabilité conjointe ont généré certaines incompréhensions ;
- la nécessité de l'autorisation du responsable du traitement initial en cas de réutilisation de données par un sous-traitant a été contestée par certains contributeurs ;
- des interrogations ont été soulevées sur les différents régimes de responsabilité des fournisseurs de SDK en fonction des spécificités de leur outil ;
- certains contributeurs ont pu comprendre que la CNIL actait une absence de responsabilité au titre du RGPD des fournisseurs d'OS et de magasins d'applications ;
- certains contributeurs ont soulevé des difficultés à mettre en œuvre les recommandations en pratique, au regard des rapports de force entre les différents acteurs visés.

Éléments de réponse de la CNIL

La CNIL a apporté plusieurs clarifications dans la recommandation finale :

- des modifications rédactionnelles ont été apportées pour clarifier les situations de responsabilité conjointe et les conditions dans lesquelles les sous-traitants peuvent traiter les données pour leurs propres finalités ;
- des clarifications ont également été apportées concernant la qualification des fournisseurs de SDK lorsque les opérations de lecture et/ou d'écriture qu'ils réalisent servent, d'une part, les finalités poursuivies par l'éditeur pour lequel ils agissent en tant que sous-traitant et, d'autre part, leurs propres finalités ;
- les parties relatives aux fournisseurs d'OS et aux fournisseurs de magasins d'applications ont été clarifiées **afin qu'elles ne puissent pas être interprétées comme une absence de responsabilité des fournisseurs d'OS et de magasins d'applications lorsqu'ils ont également un autre rôle** (notamment celui d'éditeur d'application).

Enfin, la CNIL rappelle que l'existence de rapports de force ne figure pas parmi les critères pris en compte dans le RGPD pour les qualifications des acteurs. La recommandation, qui s'adresse à tous les acteurs participant au développement et à la fourniture d'une application mobile, a pour objectif **de responsabiliser chacun d'entre eux leur rappelant les obligations qui les concernent, notamment vis-à-vis de leurs partenaires.**

À ce titre, **la CNIL est susceptible de prendre des mesures correctrices à l'encontre de tout type d'acteur, quelle que soit sa taille**. Elle veillera à procéder à une **régulation équilibrée** en tenant compte

des réalités opérationnelles, économiques et techniques d'un secteur, tout en assurant une protection effective des droits et libertés des utilisateurs.

Sur les systèmes de permission et leur articulation avec la collecte du consentement

Synthèse des contributions

Les recommandations relatives aux permissions mises en place par les fournisseurs d'OS ont fait l'objet de nombreuses remarques.

Celles-ci ont, en particulier, porté sur la proposition permettant le recueil d'un consentement valable, à certaines conditions, via les fenêtres de permission. Cette proposition a été perçue comme donnant une portée juridique à un outil technique, sans laisser un contrôle suffisant aux éditeurs d'applications sur les modalités de recueil du consentement.

Les contributeurs ont par ailleurs émis des réserves sur **l'articulation entre fenêtres de recueil du consentement et fenêtres de permissions :**

- ils considèrent que ces recommandations peuvent avoir des conséquences négatives potentielles sur l'expérience utilisateur ;
- ils estiment que la position de la CNIL conduit à faire prévaloir les fenêtres de permissions sur les fenêtres de recueil du consentement, pourtant plus spécifiques et adaptées pour recueillir le consentement.

Éléments de réponse de la CNIL

La CNIL a choisi d'encourager un ensemble de bonnes pratiques des fournisseurs de systèmes d'exploitation et des magasins d'applications pour participer au développement d'environnements plus respectueux de la vie privée, en tirant profit de leur rôle important dans l'écosystème.

À cet égard, elle réaffirme l'intérêt des permissions en tant que moyen pour les utilisateurs de protéger leur vie privée, en leur offrant plus de modalités de contrôle sur leurs données.

Cependant, la CNIL a choisi de recentrer ses recommandations sur les permissions dites « techniques » : ainsi, seules les permissions visant à donner ou bloquer l'accès à certaines ressources protégées sur leur appareil sont visées dans la version finale de la recommandation. Elle rappelle également que les permissions ne doivent pas conduire à favoriser les applications que le fournisseur d'OS a conçues ou préinstallées ; elles doivent être présentées de la même manière que pour toute autre application.

Le projet de recommandation initial proposait la possibilité de recueillir conjointement le consentement et la permission au sein d'une même fenêtre. Cette bonne pratique, qui ne se relevait pas d'une obligation légale, semblait pertinente dans des cas où des modifications mineures sur les fenêtres de permissions auraient suffi à recueillir également un consentement valide, limitant ainsi la sollicitation de l'usager. Toutefois, la CNIL a choisi de ne plus faire mention de cette pratique, dans la mesure où aucune partie prenante n'y semblait favorable.

Des modifications ont été apportées à la version finale de la recommandation afin de préciser l'articulation pratique entre permissions et recueil du consentement :

- elle souligne que les permissions peuvent être demandées dans des situations où le consentement n'est pas nécessaire et inversement ;
- elle présente la manière dont s'articulent consentement et permission lorsque les deux sont requis.

Recommandations spécifiques aux éditeurs d'applications

Synthèse des contributions

Dans la rédaction initiale du projet de recommandation, la CNIL **recommandait à l'éditeur de n'imposer la création d'un compte à l'utilisateur qu'en cas de nécessité** et d'envisager des alternatives pour éviter de collecter les adresses de courriel et mots de passe des utilisateurs.

Cette recommandation a suscité des craintes de la part des contributeurs, qui ont rappelé que la création d'un compte pouvait parfois être essentielle. Ils ont souligné la nécessité d'assurer une cohérence avec les travaux du Comité européen de la protection des données (CEPD) en cours sur le sujet.

Éléments de réponse de la CNIL

En l'absence de possibilité de préciser davantage la position de la CNIL et compte tenu des travaux du CEPD en cours sur le sujet, cette mention a été supprimée de la recommandation. La CNIL invite toutefois les acteurs à suivre leur avancée.

Recommandations spécifiques aux développeurs d'applications

Synthèse des contributions

Certaines contributions ont indiqué que les recommandations **semblaient donner un rôle excessif aux développeurs, notamment en termes de conseil aux éditeurs**.

À l'inverse, certains éditeurs ont exprimé **la crainte que les développeurs se fondent sur la recommandation de la CNIL pour ne pas suivre certaines de leurs instructions**.

De plus, les recommandations formulées par la CNIL pour la sélection des SDK ont été considérées comme trop complexes à mettre en œuvre, en partie du fait du manque de coopération de la part de certains fournisseurs de SDK. En effet, les éditeurs soulignent que ces derniers ne répondent pas systématiquement aux demandes d'information nécessaires pour mener à bien cette démarche de sélection.

Éléments de réponse de la CNIL

Les développeurs sont un des acteurs clefs de la conformité : leurs choix techniques sont susceptibles d'avoir de forts impacts sur les traitements de données personnelles qui seront mis en œuvre par l'éditeur. Les recommandations ont pour objectif **de leur permettre de mieux appréhender l'impact de leurs choix et leur permettre de participer, activement, à la conformité des applications qu'ils développent**. Elles donnent, par ailleurs, **les outils pertinents pour cadrer la relation entre l'éditeur et le développeur afin que chacun soit conscient de ses obligations respectives**.

La CNIL est consciente que certains fournisseurs de SDK ne mettent pas toujours à disposition les informations suffisantes pour mener à bien cette analyse. **La section relative aux SDK donne donc des recommandations précises afin de rendre la sélection plus aisée pour les développeurs.** Elle invite les développeurs à prendre connaissance de cette section afin d'identifier les attentes raisonnables qu'ils peuvent avoir vis-à-vis de leurs partenaires.

Recommandations spécifiques aux fournisseurs de SDK

Synthèse des contributions

Plusieurs contributeurs ont relevé qu'il était **difficile d'identifier quelles recommandations étaient applicables aux fournisseurs de SDK en fonction de leur qualification** et des traitements considérés.

En particulier, certaines contributions se sont interrogées sur les obligations qui pèsent sur les fournisseurs de SDK qui n'agissent que comme sous-traitants, et qui n'utilisent pas les données personnelles pour des finalités qui leurs sont propres.

Éléments de réponse de la CNIL

La recommandation finale a été modifiée pour **mieux distinguer les obligations applicables ainsi que les recommandations pour s'y conformer en fonction de la qualification du fournisseur de SDK dans les traitements de données personnelles mis en œuvre**.

La CNIL souligne que :

- dans les pratiques actuelles du marché, la qualification de « sous-traitant » pour un fournisseur de SDK est moins fréquente que celle de « responsable » ou de « responsable conjoint » de traitement.
- lorsque le fournisseur de SDK est uniquement « sous-traitant », il doit fournir au responsable du traitement les informations et documentations nécessaires pour assurer la conformité des traitements de données mis en œuvre.

Dispositifs de signalement et score de vie privée au sein du magasin d'applications

Synthèse des contributions

La suggestion initiale de la CNIL de **mettre en œuvre un système de score relatif à la prise en compte de la vie privée des utilisateurs**, par analogie avec le NutriScore pour les denrées alimentaires, a fait l'objet de nombreuses observations de la part de plusieurs catégories d'acteurs distinctes mais également de l'Autorité de la concurrence.

Ces observations portaient sur les méthodologies de définition de ce score, son implémentation pratique par les magasins d'applications ainsi que sa compatibilité en principe et en pratique vis-à-vis du récent paquet numérique européen, notamment le règlement sur les marchés numériques (*Digital Markets Act*, ou DMA).

Plusieurs acteurs ont, par ailleurs, exprimé des craintes concernant **le mécanisme de signalement des applications au sein des magasins d'applications prévu dans la recommandation**. Les contributeurs ont ainsi pointé un risque de chevauchement avec le dispositif consacré par le règlement sur les services numériques (*Digital Services Act*, ou DSA).

Éléments de réponse de la CNIL

La CNIL a fait évoluer sa recommandation afin notamment de souligner que le score de vie privée devrait reposer sur une méthodologie préalablement définie, de manière transparente, **par un acteur tiers** au fournisseur de magasin d'applications. Elle a également supprimé certains exemples, considérant que les critères nécessitent une réflexion plus poussée et coconstruite avec les diverses parties prenantes.

La CNIL a précisé que les dispositions concernant le dispositif de signalement – qui se limitent par ailleurs à des bonnes pratiques – **s'inscrivent bien dans le cadre du dispositif de signalement prévu par le DSA**, ce qui exclut tout risque de chevauchement.

Documents de référence

- « La loi Informatique et Libertés », cnil.fr
- « Le règlement général sur la protection des données (RGPD) », cnil.fr
- La recommandation de la CNIL sur les applications mobiles (PDF, 3,1 Mo), cnil.fr