# Projet de recommandation relative aux applications mobiles – CNIL

## Contribution à la consultation publique

## Alliance Digitale

### Introduction

Alliance Digitale est la principale association professionnelle des acteurs du marketing digital et de la publicité en ligne en France. Elle est issue du rapprochement de l'IAB France et de la Mobile Marketing Association France.

L'association regroupe la grande majorité des acteurs du marketing digital en France, soit près de 250 entreprises réparties sur l'ensemble de la chaîne de valeur (Marques, Médias, Agences, Régies, Plateformes, Tech, Places de marchés etc.).

Elle rassemble également une grande partie des acteurs des écosystèmes mobiles auxquels le projet de recommandation de la CNIL s'adresse. Alliance Digitale a donc vocation à répondre, dans le cadre de la consultation publique organisée par le CNIL, à l'ensemble des éléments couverts par le projet de recommandation.

Nous accueillons favorablement cette démarche de la CNIL visant à aider les professionnels du mobile dans leur conformité à la réglementation relative à la protection des données personnelles.

Alliance Digitale s'est mobilisée depuis le début des travaux initiés par la CNIL. Nous avons notamment été auditionnés le 13 décembre 2022 par les services en charge du dossier et avons répondu à la consultation publique sur les enjeux économiques de la collecte de données sur mobile en février dernier.

Nous regrettons néanmoins que les consultations du secteur n'aient pas été plus importantes. Lors de notre audition le 13 décembre, nous avions déjà signalé que les consultations préliminaires effectuées par la CNIL auprès d'une vingtaine d'acteurs représentatifs du marché nous semblaient insuffisantes pour bien appréhender les spécificités du marché.

Nous regrettons également que la CNIL se soit engagée dans une démarche unilatérale de production de normes interprétatives quand elle aurait pu privilégier une approche inclusive de spécification des règles telle que celle offerte par les codes de conduite[1]. Cette méthode aurait en effet été plus adaptée à la spécificité et la complexité du secteur des applications mobiles. Elle aurait aussi permis une continuité des échanges et une meilleure compréhension des problématiques du secteur et de ses enjeux de concurrence et d'innovation.

Par ailleurs, nous avons été surpris d'observer que l'essentiel des points qui ont été remontés par Alliance Digitale et notamment par le biais du questionnaire sur les enjeux économiques n'ont pas été pris en compte dans ledit projet de recommandation.

Cependant, nous sommes satisfaits de voir que la CNIL a saisi formellement l'Autorité de la concurrence dans le cadre de ce projet de recommandation. La prise de conscience croissante de l'imbrication des enjeux de protection des données personnelles et de concurrence impose une collaboration soutenue et pérenne entre les deux autorités.

Nous espérons que la recommandation saura non seulement tenir compte de la situation concurrentielle tout à fait spécifique du secteur des applications mobiles mais également être totalement neutre du point de vue de ses impacts sur la concurrence entre les différents acteurs. Il est à ce titre indispensable que la recommandation de la CNIL ne permette pas de légitimer les pratiques abusives (et potentiellement illicites) des fournisseurs de systèmes d'exploitation et de magasins d'applications.

Vous trouverez ci-dessous la réponse de Alliance Digitale à la consultation publique. Celle-ci s'organise sur la base de remarques générales et de remarques spécifiques qui suivent l'organisation du projet de recommandation.

**Synthèse et demandes**

Le projet de recommandation soulève de nombreuses interrogations et inquiétudes pour l'ensemble des membres de Alliance Digitale. Dans cette réponse à la consultation publique nous alertons la CNIL principalement sur :

- Les risques d'incompréhension qui pourraient émerger du fait de longueur, de la complexité et du niveau de détail fourni dans le projet, ce qui pourrait décourager les acteurs de s'y référer et donc, avoir un effet contre-productif ;

[1] Articles 40 et suivants du RGPD et article 8 2 (b) de la Loi Informatique et Libertés du 6 janvier 1978. En sus, l'article 57(1)m du RGPD prévoit d'ailleurs que les autorités de protection des données personnelles et donc la CNIL ont pour tâche d'encourager l'élaboration de codes de conduite.

- L'absence de sécurité juridique apportée aux acteurs par ce projet tant il soulève davantage de questions qu'il n'apporte de réponses ;

- La confusion quant à la valeur juridique des dispositions présentes au sein du projet de recommandation, à savoir si elles relèvent d'obligations légales, de bonnes pratiques du marché ou de simples recommandations du régulateur ;

- Le caractère prescriptif du document qui tente de capturer l'intégralité des situations en fonction des différents acteurs plutôt que de fixer des grands principes, ce qui risque de créer une réticence des acteurs à innover ;

- Les nombreuses obligations/recommandations découlant d'une surinterprétation des textes et/ou ne considérant pas les autres réglementations applicables aux acteurs du marché des applications mobiles ;

- Le renforcement de la position dominante d'acteurs verticalement intégrés du fait de la non prise en compte de la situation concurrentielle spécifique du marché des applications mobiles ;

- La validation et la légitimation du rôle de prescripteur de règles en matière de protection des données des fournisseurs d'OS et de magasins d'applications et le déséquilibre que cela engendre entre les prérogatives qui leur sont octroyées et les faibles responsabilités qui leur sont imputées ;

- La création par la CNIL d'une situation de désavantage concurrentiel sur le marché pour les acteurs dont la elle est l'autorité cheffe de file.

Dans ce cadre et à l'aune des éléments présentés ci-dessus, nous souhaiterions que la CNIL soit en mesure de :

- Rendre public l'avis de l'Autorité de la concurrence ;

- Rendre transparente la consultation publique :

    - Publier sur le site de la CNIL l'ensemble des contributions reçues à la manière dont l'EDPB procède depuis plusieurs années[2] ;

[2] Exemple : Recommendations 1/2022 on the Application for Approval and on the elements and principles to be found in Controller Binding Corporate Rules (Art. 47 GDPR) | European Data Protection Board (europa.eu)

- Fournir un compte-rendu exhaustif et détaillé des contributions reçues lors de la consultation publique. Ledit compte-rendu devrait également expliquer pour chacun des points remontés par les contributeurs et au sein de l'avis de l'Autorité de la concurrence les raisons pour lesquelles ils sont retenus ou écartés dans la recommandation finale de la CNIL ;

- Publier une version amendée du projet de recommandation soumise à une nouvelle consultation auprès des acteurs pertinents dans les prochains mois. C'est une démarche nécessaire pour Alliance Digitale au regard des nombreuses problématiques soulevées et des implications concurrentielles massives dudit projet ;

- Scinder cette version amendée soumise à consultation en deux documents distincts :

  - Des lignes directrices concises et contraignantes ;

  - Des recommandations proposant des modalités pratiques non-limitatives pour guider l'ensemble des parties prenantes de l'écosystème mobile dans leur propre analyse réglementaire et pratique.

## I. Remarques générales

- **Sur la lisibilité et la durée dans le temps du projet de recommandation**

Le projet de recommandation relative aux applications mobiles s'étend sur presque 100 pages. A titre de comparaison, les documents publiés le 17 septembre 2020 concernant les lignes directrices et recommandations de la CNIL relatives aux « cookies et autres traceurs » ne comprennent que 24 pages à eux deux[3]. En outre, l'avis du G29 sur les applications mobiles et les smartphones adopté le 27 février 2013[4] et sur lequel la CNIL s'est inspirée pour ledit projet de recommandation ne fait que 30 pages. Le parti pris des rédacteurs de ce projet de recommandation semble différent des documents mentionnés ci-avant : il s'agit en l'espèce de fournir un niveau de détail important aux acteurs du marché avec pour objectif d'être le plus complet possible voire d'être exhaustif. Il est ainsi intéressant de noter à ce titre que, dans le cadre du questionnaire de la consultation publique, la CNIL souhaite s'assurer que les

[3] https://www.cnil.fr/fr/cookies-et-autres-traceurs/regles/cookies/lignes-directrices-modificatives-et-recommandation

[4] G29 WP 202 Opinion 02/2013 on apps on smart devices, adopté le 27 février 2013 https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf

acteurs disposent bien d'un niveau de détail suffisant pour mener à bien leurs travaux de conformité[5].

S'il faut saluer les efforts entrepris pour fournir le niveau de détail présent dans le projet de recommandation, nous souhaitons alerter la CNIL quant aux effets pervers de cette approche en matière de lisibilité, d'accompagnement de l'innovation et de durée dans le temps[6].

Il nous semble tout d'abord que cette méthode est **inadaptée à l'écosystème auquel le projet de recommandation est destiné**. L'environnement mobile se caractérise par la présence de nombreuses petites et moyennes entreprises -à l'exception évidente des fournisseurs de magasins d'applications et de systèmes d'exploitation- qui n'ont pour la plupart pas ou peu de ressources pour analyser et comprendre ce type de document. Il nous paraît impératif que ce type de communication de la CNIL soit accessible, facile à lire et se concentre en priorité sur les grands principes directeurs de la réglementation avec quelques illustrations concrètes et non exhaustives. Une telle approche permettrait davantage à l'ensemble des acteurs -indépendamment de leur taille- de comprendre les implications du RGPD pour leurs activités. A ce stade, nous estimons que cet objectif d'exhaustivité nuit non seulement à l'exercice de simplification et de clarification du droit applicable mais également à l'accompagnement de l'innovation des acteurs de l'écosystème, mission figurant comme l'une des principales de la CNIL[7]. Nous estimons ainsi que le projet de recommandation ne répond pas suffisamment à l'objectif poursuivi d'apporter de la sécurité juridique au marché et, en sus, par sa longueur et complexité, est de nature à créer de nouvelles interrogations.

De la même manière, nous sommes inquiets quant à la **capacité de ce type de document de résister à l'épreuve des changements technologiques**. L'environnement numérique et les technologies associées évoluant particulièrement rapidement, nous pensons que beaucoup de détails fournis risquent de ne plus être pertinents prochainement. A titre d'exemple, les tableaux de synthèse des vérifications fournis en conclusion de chaque partie avec les différents points de contrôle au cas par cas peuvent s'avérer utiles mais nous paraissent, dans l'ensemble, trop détaillés. Il pourrait être utile de les simplifier pour faciliter la lecture et la compréhension en ne conservant que les principales vérifications à mener. De plus, ces documents n'indiquent pas aux acteurs si ces vérifications sont suffisantes pour assurer leur conformité ou dans quelle mesure le respect de ces points de contrôle pourrait constituer un facteur permettant de réduire le montant d'une éventuelle amende le cas échéant.

---

[5] Voir première question de chaque partie. Exemple pour la partie éditeurs : « *Les recommandations visant à encadrer les relations entre l'éditeur et ses partenaires sont-elles suffisamment détaillées ? Des situations supplémentaires nécessiteraient-elles d'être abordées ? si oui, lesquelles ?* »

[6] *Future-proofness*

[7] https://www.cnil.fr/sites/cnil/files/attachment_533_102.pdf

Pour s'assurer que le document résiste à l'épreuve du temps, nous recommandons à la CNIL d'instaurer un dialogue fréquent et inscrit dans la durée avec l'ensemble des acteurs économiques. Cette approche ne nous semble pas envisageable dans le cadre du présent projet. Néanmoins, le dialogue pourrait être facilité dans le cadre de la mise en place d'un code de conduite ou via la publication de référentiels dédiés aux enjeux les plus spécifiques.

Enfin, s'il est indiqué que le projet de recommandation « s'adresse particulièrement aux délégués de la protection des données[8]», nous estimons que le document traite également d'enjeux purement techniques et que de ce fait, va devoir également être lu et compris par des profils techniques. Afin de limiter le risque d'interprétations diverses voire contradictoires entre ces deux types de profil, nous recommandons à la CNIL de s'inscrire dans la continuité de ce qu'elle avait fait jusqu'ici sur les cookies et autres traceurs, à savoir de fournir des communications distinctes pour les développeurs et pour les DPO/juristes[9].

- **Sur la segmentation par type d'acteurs du projet de recommandation**

Le projet de recommandation distingue (1) des éléments généraux relatifs à son périmètre et à la qualification des acteurs et (2) des dispositions spécifiques destinées à cinq catégories d'acteurs : les éditeurs d'applications, les développeurs, les fournisseurs de SDK, les fournisseurs de systèmes d'exploitation et les fournisseurs de magasins d'applications.

Il s'agit d'une segmentation intéressante qui pourrait en théorie faciliter la lecture en permettant aux différents acteurs de ne prendre connaissance que de la partie qui leur est dédiée, en plus des parties introductives concernant l'entièreté du marché. En pratique, le projet de recommandation ne le permet pas. Les renvois vers d'autres communications de la CNIL, du CEPD ou de l'ICO -dont la portée contraignante ou non n'est pas claire- sont nombreux, notamment dans les parties dédiées aux différents acteurs : **le projet de recommandation ne peut donc être considéré comme un document réellement autonome**, ce qui accentue les problèmes de lisibilité et clarté mentionnés ci-dessus.

Par ailleurs, les parties dédiées aux acteurs ne sont pas non plus autonomes. Il n'est par exemple par possible pour un éditeur d'application de ne lire que la partie qui lui est dédiée au risque de passer à côté d'éléments importants « susceptibles de le concerner de manière incidente[10] ». A titre d'exemple, de nombreuses obligations structurantes imposées aux éditeurs d'applications (gestion des permissions, partage de données avec les magasins

[8] Page 5 du projet de recommandation
[9] Exemple du Guide RGPD pour l'équipe de développement destiné aux développeurs et des lignes directrices « Cookies et autres traceurs » à l'attention des DPO et juristes d'entreprise.
[10] Page 5 du projet de recommandation

d'applications, référencement des applications etc.) ne sont précisées que dans les parties dédiées aux systèmes d'exploitation ou aux magasins d'applications.

Deux mesures pourraient être envisagées pour répondre aux problématiques ci-dessus : (1) revoir complètement la structure du document et abandonner l'approche basée sur les différents acteurs ou (2) garantir que chaque partie du projet de recommandation puisse être consultée de manière autonome.

- **Sur la nécessaire clarification entre ce qui relève de l'obligation et ce qui est de l'ordre de la recommandation ou de la bonne pratique**

Le projet de recommandation entretient un flou particulièrement problématique entre ce qui relève de l'obligation réglementaire et ce qui relève de la bonne pratique ou de la recommandation. Aucune démarcation claire n'est tracée dans le projet de recommandation. L'analyse et l'interprétation du droit applicable est mélangée tout au long de la lecture à ce qui semble plutôt relever de recommandations émises par la CNIL, lesquelles peuvent être ou non basées sur des pratiques de marché. Cela engendre une **confusion généralisée parmi les parties prenantes**, de nature à susciter de nouvelles interrogations alors même que le projet de recommandation est destiné à répondre aux questionnements des différents acteurs. Nous reviendrons sur certains exemples dans les parties spécifiques dédiées aux différentes parties prenantes.

Il est essentiel que le projet de recommandation exprime clairement cette distinction entre les obligations d'un côté et les recommandations de l'autre. Il y a ainsi des obligations, qui ont force contraignante. Celles-ci doivent être justifiées et reposer sur une base légale claire. Quant aux recommandations, elles ne sont destinées qu'à aider les professionnels dans leur démarche de mise en conformité et reflètent généralement l'opinion du régulateur sur les actions qui pourraient être menées par les entreprises dans le cadre de ladite démarche. Elles ne servent qu'à des fins d'exemples et doivent clairement indiquer qu'elles ne sont pas limitatives et que d'autres approches sont envisageables.

Par conséquent, nous suggérons à la CNIL de scinder son projet de recommandation en deux documents distincts : des lignes directrices concises et contraignantes d'un côté et des recommandations proposant des modalités pratiques non-limitatives pour guider l'ensemble des parties prenantes de l'écosystème mobile dans leur propre analyse réglementaire et pratique de l'autre.

- **Sur l'interaction du projet de recommandation avec la réglementation existante**

Le projet de recommandation nous apparait ne pas tenir suffisamment compte de **l'articulation et de la coexistence du RGPD et de la Loi Informatiques et Libertés avec d'autres réglementations en vigueur**. Ledit projet est construit comme s'il opérait en vase clos, sans tenir compte d'autres réglementations applicables aux acteurs du mobile, et néglige l'opportunité de clarifier leur articulation avec la réglementation en matière de protection des données personnelles. Cette situation conduit à des chevauchements et contradictions nombreux avec certains instruments juridiques en vigueur qui compromettent la solidité juridique dudit projet et la sécurité juridique des acteurs qui y seront tenus.

Si nous revenons en détail tout au long de notre réponse sur les chevauchements inutiles et contradictions inquiétantes que nous avons pu observer, nous souhaitons mettre certaines en exergue ici, notamment les tensions créées avec le paquet Digital Markets Act (DMA) / Digital Services Act (DSA) et le droit de la consommation.

En ce qui concerne l'articulation avec le **DMA**, nous alertons sur plusieurs dispositions qui viennent notamment forcer les éditeurs d'applications à partager des informations avec des entreprises désignées comme « gatekeepers » sur le fondement de l'article 3 du texte et qui sont contraires à l'esprit et à la lettre du texte. Pour ce qui est du **DSA**, le projet de recommandation vient créer un mécanisme de signalement pour les utilisateurs concurrent de celui prévu à l'article 14 du texte, sans en préciser son utilité et sa coexistence avec celui-ci[11].

Le projet de recommandation néglige par ailleurs d'explorer les instruments juridiques applicables au droit des consommateurs pour les acteurs des applications mobiles. Il aurait été pertinent par exemple d'inclure les directives sur les droits des consommateurs, notamment la directive Omnibus 2019/2161, qui envisage un service ou un contrat en contrepartie de la fourniture et de l'utilisation de données personnelles.

De ce fait, nous appelons la CNIL à revoir certains éléments de son projet de recommandation à l'aune de la coexistence et de l'articulation avec la réglementation existante afin d'apporter la sécurité juridique recherchée aux acteurs concernés et renforcer la solidité légale dudit projet.

[11] Partie 9.3, page 89 du projet de recommandation.

- **Sur l'insuffisance prise en compte de la situation concurrentielle sur le mobile**

Le projet de recommandation est destiné à apporter une aide à l'ensemble des acteurs du marché quant à la mise en conformité avec la Loi Informatique et Libertés et le RGPD. Son rôle est donc de clarifier les obligations de chacun en l'état actuel du droit. Ce travail doit être neutre d'un point de vue concurrentiel, c'est-à-dire qu'il ne doit pas favoriser un type d'acteur plutôt qu'un autre ou aggraver une situation économique déjà singulièrement inégalitaire. C'est d'autant plus important que le mobile constitue une part essentielle du trafic Internet des Français[12] et que les applications comptent pour 89% du temps passé sur un téléphone[13].

Il apparait que le projet de recommandation fait fi de de la situation concurrentielle des marchés du mobile. Cette situation dans laquelle s'exercent des rapports de force particulièrement déséquilibrés entre les différents acteurs [14] n'est que très brièvement mentionnée [15] et n'est pas prise en compte dans l'explication des obligations et recommandations. Le projet donnerait presque l'impression aux lecteurs qu'il existe autant de fournisseurs de magasins d'applications que de développeurs, ou autant de fournisseurs de systèmes d'exploitation que d'éditeurs d'applications. Si le projet de recommandation reconnait bien que les tiers ne peuvent s'adresser qu'à Apple dans l'environnement iOS, il surestime largement l'influence des systèmes d'exploitation et magasins d'applications tiers sur l'environnement Android. Pour rappel, les magasins d'applications d'Android et iOS représentent entre 95 et 100% de l'ensemble des téléchargements [16] et leurs systèmes d'exploitation comptent pour 100% des parts de marchés (respectivement 79% pour Android et 21% pour Apple iOS[17]).

Il ne s'agit pas de revenir ici sur les descriptions que nous avons pu apporter lors de notre réponse au questionnaire de la CNIL sur les enjeux économiques de la collecte de données mobiles. Pour autant, nous sommes inquiets de voir que le projet de recommandation ne tient absolument pas compte de la singularité concurrentielle du marché. Aucune prise en compte des rapports asymétriques qui prévalent entre les fournisseurs de magasins d'applications/systèmes d'exploitation et les tiers n'est relevée. L'impact de leurs décisions sur le reste de l'écosystème n'est pas non plus appréhendé. Aucune mention du fait qu'une seule et même entreprise peut être aussi bien fournisseurs de systèmes d'exploitation, de

[12] 75% du trafic en France se fait sur smartphone, Médiamétrie, 2022 : https://www.mediametrie.fr/fr/lannee-internet-2022
[13] AppNanie, 2021, https://www.data.ai/en/go/state-of-mobile-2021/
[14] Market Study Report on Mobile OS and Mobile App Distribution position, Japan Fair Trade Commission, 9 février2023 https://www.jftc.go.jp/en/pressreleases/yearly-2023/February/230209.html
[15] P. 21 du projet de recommandation relatif aux applications mobiles
[16] Mobile ecosystems market study final report, Competition Market Authority, June 2022 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1096277/Mobile_ecosystems_final_report_-_full_draft_-_FINAL__.pdf
[17] Ibid.

magasin d'applications, de SDK que d'éditeurs d'applications [18] n'est envisagée. Autant d'éléments qui sont largement vérifiés par la littérature économique, font l'objet d'une vigilance accrue des régulateurs[19] et que nous vous avions largement partagés dans le cadre de notre réponse au questionnaire sur les enjeux économiques.

Si la concurrence ne relève pas par elle-même du périmètre d'action de la CNIL, elle devrait tenir une position plus nuancée, tenant compte de l'articulation des rôles et des responsabilités sur le marché, au besoin en sollicitant l'expertise de l'Autorité de la concurrence sur ces sujets. Sans cette prise en compte nécessaire, nous craignons que la recommandation de la CNIL ne vienne aggraver une situation déjà inégalitaire et renforcer le rôle de « gatekeepers » des acteurs dominants au détriment du reste de l'écosystème du mobile.

- **Sur le risque de voir le projet de recommandation renforcer les déséquilibres à l'œuvre sur le marché**

Au-delà de l'absence de prise en compte du caractère concurrentiel, nous craignons que le projet de recommandation ne renforce les nombreux déséquilibres à l'œuvre. L'orientation globale dudit projet nous parait favoriser très largement les grands acteurs à savoir les deux fournisseurs de magasins d'applications et de systèmes d'exploitation dominants, au détriment des acteurs tiers. Si nous reviendrons en détail dans la suite de notre réponse avec des exemples spécifiques, il s'agit ici de répertorier trois éléments principaux qui nous font craindre une aggravation majeure des déséquilibres.

Le premier élément relève du **partage des obligations et des responsabilités au sein de la chaine de valeur**. Le projet de recommandation vient ajouter de nombreuses nouvelles obligations à l'ensemble des acteurs de la chaîne de valeur, tout particulièrement aux éditeurs d'applications, ce qui pourrait avoir la conséquence de créer un environnement concurrentiel plus restrictif en France qu'ailleurs en Europe. A contrario, les obligations nouvelles à destination des fournisseurs de magasins d'applications et de systèmes d'exploitation sont minimales pour ne pas dire inexistantes et leurs responsabilités dans l'écosystème particulièrement limitées. Cela va nécessairement conduire à une concentration accrue des données entre un nombre très limité d'acteurs essentiellement verticalement intégrés.

[18] Voir Réponse AD au questionnaire sur les enjeux économiques de la collecte de données sur mobile *« Très concrètement, les magasins d'applications jouent non seulement le rôle de magasins mais aussi de fournisseurs de produits, de collecteurs de données, de fournisseurs de solutions marketing et publicitaires ou encore de pourvoyeurs d'infrastructures de paiement sans oublier de régulateurs* »

[19] Voir récente ouverture d'une étude sur les écosystèmes mobiles par la Commission européenne : https://www.reuters.com/technology/eu-study-mobile-ecosystems-counter-any-apple-google-antitrust-pushback-2023-10-04/

Le deuxième élément correspond **au rôle des fournisseurs de magasins d'applications et de systèmes d'exploitation dans la mise en conformité du reste des acteurs du marché**. Le projet de recommandation fait de ceux-ci le bras armé du régulateur pour assurer la conformité des acteurs du marché. Cela pose plusieurs problématiques importantes :

- Premièrement, la CNIL, avec ces recommandations, vient entériner un état de fait qui n'était jusque-là que la conséquence de la position dominante des fournisseurs de magasins d'applications et de systèmes d'exploitation, à savoir celui de **prescripteur de pratiques en matière de protection des données personnelles**. Nous nous inscrivons en opposition ferme contre ce principe, comme nous l'avons d'ailleurs indiqué dans le cadre de notre réponse au questionnaire sur les enjeux économiques de la collecte de données mobiles, le rôle d'un fournisseur de magasins d'applications, ou de systèmes d'exploitation n'est pas de se substituer au régulateur et encore moins au législateur. De la même manière, le régulateur n'est pas censé faire reposer une partie du mandat qui lui est confié par la loi sur un ou plusieurs types d'acteurs.

- Dans le même esprit, le projet de recommandation vient également entériner toute une série de pratiques déjà appliquées par les fournisseurs de magasins d'applications et de systèmes d'exploitation, et tout particulièrement celles d'Apple. La CNIL vient ici ainsi légitimer toutes une série de pratiques qui ne relèvent pas d'un accord librement consenti avec les acteurs de l'écosystème mais d'une **collaboration obligatoire sous la contrainte**. De la même façon, elle légitime toutes les pratiques futures qui pourraient être mises en place par les fournisseurs de magasins d'applications et de systèmes d'exploitation, et ce quelles qu'en soient les conséquences économiques sur le reste de l'écosystème. De ce fait, la CNIL octroie un avantage concurrentiel additionnel aux entreprises dominantes verticalement intégrées comme Apple dont les applications et SDK propres sont en concurrence avec le reste de l'écosystème. Dans cette démarche, la CNIL se place en complète contradiction avec le mandat de l'Autorité de la concurrence d'éviter les pratiques abusives des acteurs dominants.

- Enfin, le projet de recommandation vient, par la constitution deux environnements distincts d'obligations pour des services similaires, à l'exception de ceux des *walled-gardens* **rompre le principe de neutralité technologique**. Pour répondre aux obligations du document, notamment en matière de permissions, les éditeurs d'applications vont devoir créer des services distincts entre les environnements desktop et mobile, collecter le consentement sur chaque appareil tandis que les *walled-gardens* vont toujours pouvoir se reposer sur un consentement global de l'utilisateur lors de son inscription, *a fortiori* dans une logique cross-device (applications, web mobile, desktop, télé connectée etc.). Ce faisant, la CNIL vient renforcer une distorsion de concurrence entre les différents acteurs de la chaîne de valeur.

- **Sur l'introduction de nombreuses obligations de conseil pour les différents acteurs**

Le projet de recommandation fait de nombreuses références au « devoir de conseil » à l'instar de celui conféré aux fournisseurs de magasins d'applications[20] ou encore aux développeurs[21].

Si le RGPD prévoit des obligations d'aide, notamment du sous-traitant au responsable de traitement[22], la notion de « devoir de conseil » n'existe pas telle quelle. Ceux qui disposent de missions de conseil dans le RGPD sont uniquement les délégués à la protection des données[23] et les autorités de contrôle[24].

Par ailleurs, la notion de « devoir de conseil » est avant tout un concept de droit civil[25] dont la définition des contours est exclusivement dévolue aux tribunaux civils sous le contrôle de la Chambre Civile de la Cour de cassation. Il n'appartient donc pas à la CNIL d'apporter des prescriptions précises sur ce sujet, mais de laisser les parties mettre en œuvre cette obligation dans les limites prévues par les textes et sous le contrôle des juridictions civiles. Tout autre approche porterait atteinte au principe fondamental de la liberté contractuelle des parties.

[20] Partie 9.2.1 page 88 du projet de recommandation.
[21] Partie 6.2 page 48 du projet de recommandation
[22] Article 28 (f) du RGPD
[23] Article 39 du RGPD
[24] Article 58 du RGPD
[25] Article 1112-1 du Code Civil

## II. Remarques spécifiques

La présente partie revient sur les points les plus problématiques que Alliance Digitale a pu relever. Elle reprend l'organisation du projet de recommandation.

### Concernant le périmètre de la recommandation et le rôle de chaque acteur dans le cadre de l'utilisation de l'application

- Sur l'exemption domestique

La troisième partie du projet de recommandation revient sur le principe de « l'exemption domestique » sur la base de l'article 2.2.c et du considérant 18 du RGPD. Si nous accueillons favorablement cette précision liminaire, certains éléments pourraient être éclaircis.

Le passage du régime d'exemption au régime normal ne nous semble pas assez clairement défini dans le projet de recommandation. Voici quelques questions que nous nous posons à la lecture de cette partie :

- Quand la bascule d'un régime à l'autre s'opère-t-elle ?
- Est-ce à partir du moment où les informations ne sont plus stockées dans le terminal de l'utilisateur et/ou à partir du moment où un tiers peut avoir accès à ces informations ?
- Est-ce lorsqu'une personne physique nécessite les moyens techniques d'un tiers pour le traitement ?
- Est-ce dès lors qu'il y a un transfert de données personnelles ?
- Que se passe-t-il s'il n'y a pas de traitement au sens du RGPD ?

Par ailleurs, nous avons une interrogation quant à la phrase : « la CNIL **encourage vivement** le fait de proposer des applications mobiles reposant sur des traitements effectués entièrement à l'initiative et sous le contrôle de la personne selon les conditions définies ci-dessus [26]». C'est le seul et unique moment où la CNIL associe ces deux termes, il est donc difficile d'en analyser la portée juridique pour les parties prenantes. Cela renforce notre inquiétude générale concernant la confusion entourant le projet de recommandation, quant à savoir si les dispositions présentes relèvent d'obligations légales, de simples recommandations, ou de bonnes pratiques.

[26] P. 14 du projet de recommandation

- Sur la volonté de déterminer les qualifications de chaque acteur

Sur la pertinence générale du niveau de détail fourni

Le projet de recommandation consacre son quatrième chapitre aux « rôles de chaque acteur » et plus concrètement, à leur qualification au sens du RGPD. Cette partie est destinée à aider les parties prenantes à mieux tracer la ligne de partage entre les différentes qualifications.

Si le projet précise que la « qualification des acteurs doit être réalisée au cas par cas [27]», et qu'une « requalification, appréciée au regard des justifications fournies est toujours possible[28] », il consacre toute une série d'exemples très détaillés qui semblent *de facto* revêtir un caractère prescripteur. Cet exercice censé faciliter la vie des différentes parties prenantes risque d'aboutir à une situation inverse où ces dernières, dans l'hypothèse où leur analyse de la qualification différerait, au regard d'un contexte spécifique, de celles consacrées par le projet de recommandation, seraient contraintes de se justifier auprès de la CNIL.

Nous recommandons à la CNIL d'alléger cette partie et de ne fournir aux acteurs qu'un rappel des principes généraux afin de ne pas les contraindre dans leurs analyses propres qui sont évidemment tributaires de situations et modes de fonctionnement spécifiques à chacun d'entre eux.

Sur les difficultés posées par les découpages proposés

Cette partie consacre toute une série de cas d'usage pour l'ensemble des acteurs concernés et principalement pour les éditeurs d'applications, développeurs et fournisseurs de SDK. Les découpages proposés entre responsable de traitement, responsable de traitement conjoint et sous-traitant ne correspondent pas à la réalité pratique de l'écosystème mobile. Cela entrainerait l'obligation de gérer trois qualifications différentes au sens du RGPD pour un seul et même service, ce qui nous apparait inutilement fastidieux et sans intérêt pour la protection des données personnelles de l'utilisateur final. En outre, la CNIL s'appuie sur une approche abstraite selon laquelle chaque acteur serait en mesure de conclure des contrats direct et personnalisés avec chacun de ses partenaires, ce qui ne se produit pas toujours en pratique.

Pour ce qui est du cas spécifique de la qualification des fournisseurs de SDK et de leurs relations avec les éditeurs d'applications, elle nous semble poser plusieurs problématiques :

[27] P. 17 du projet de recommandation
[28] Ibid.

- Comme nous le notons ci-après dans le cadre des audits demandés[29], les éditeurs d'applications ne disposent pas nécessairement d'une relation contractuelle avec l'ensemble des fournisseurs de SDK. Par ailleurs, les éditeurs d'applications sont parfois dans un rapport de force défavorable avec certains fournisseurs de SDK. Cela peut entrainer des situations où les éditeurs ne sont pas en mesure d'obtenir un accord de sous-traitance tel que consacré dans le projet de recommandation ;

- Nous contestons la disposition selon laquelle les fournisseurs de SDK auraient l'obligation de demander l'accord préalable du responsable de traitement pour traiter les données pour leurs finalités propres. Une telle obligation n'est pas requise par le RGPD. Le fournisseur de SDK doit pouvoir réutiliser les données pour son propre compte en tant que responsable de traitement à partir du moment où ce dernier respecte l'ensemble des dispositions associées à cette qualification. Cette obligation supplémentaire qui ne correspond pas au fonctionnement actuel du marché pourrait entraver la liberté d'action et l'innovation des fournisseurs de SDK dans la réutilisation des données nécessaires à la performance et l'amélioration de leurs outils et services et ainsi, devenir un obstacle opérationnel important dans le développement et l'intégration de SDK.

- Par ailleurs, le projet de recommandation reste flou quant à la responsabilité des éditeurs d'applications dans le cas où l'accord pour réutiliser les données aurait été donné au fournisseur de SDK : que se passe-t-il si le fournisseur de SDK ne remplit pas ses obligations légales ? L'éditeur d'application qui a consenti à la réutilisation des données par le SDK serait-il également responsable ?

- Sur la (non)qualification du magasin d'applications au sens du RGPD

Il est indiqué dans le projet de recommandation que le magasin d'applications « appréhendé en tant qu'acteur édictant des règles relatives à la publication des applications au sein du magasin d'applications ne dispose pas à ce titre d'une qualification au sens du RGPD[30] ».

Ce postulat de départ nous semble être une erreur. Le magasin d'applications, même restreint à ce rôle spécifique de prescripteur de règles traite nécessairement des données personnelles des utilisateurs que ce soit pour la livraison des applications, les mises à jour, la gestion des consentements des utilisateurs dans les réglages, ou encore ses nombreuses autres interactions avec l'appareil de l'utilisateur. La CNIL semble offrir ici un traitement de faveur injustifié aux magasins d'applications. Cette position est d'autant plus surprenante que cette

[29] Voir également Question 12 de la réponse Alliance Digitale au questionnaire sur les enjeux économiques de la collecte de données mobiles.
[30] P. 22 du projet de recommandation.

dernière, en tant qu'autorité concernée dans le cadre de la procédure de coopération initiée par l'Autorité de protection des données belge (APD), a pris une position inverse en considérant que l'IAB Europe, en tant qu'acteur édictant des règles relatives au standard TCF, devait recevoir la qualification de responsable de traitement conjoint au sens du RGPD.

Enfin, si comme il est mentionné, « l'éditeur du magasin, appréhendé en tant qu'éditeur d'applications, se verra appliquer les mêmes qualifications et obligations que pour n'importe quel éditeur d'applications[31] », il est étrange de considérer qu'il dût disposer d'une catégorie à part entière dans le projet de recommandation. Cette catégorie à part entière confirme que la CNIL confie à cette catégorie d'acteurs privés à but lucratif, appartenant à des entreprises verticalement intégrées et en concurrence avec l'ensemble des autres, un rôle central dans l'application de la régulation. Conférer un tel pouvoir aux magasins d'applications représente en soi un excès de pouvoir, en les incitant à assumer des responsabilités qui relèvent normalement de la compétence du régulateur et donc en l'espèce, de la CNIL.

- Sur le principe du consentement de l'utilisateur comme base légale pour la publicité personnalisée

A plusieurs reprises dans son projet de recommandation, la CNIL indique que la seule base légale possible pour la publicité en ligne et le profilage est le consentement. Exemple page 28 du projet de recommandation : « En principe, le profilage et la publicité personnalisée ne peuvent être justifiés par l'intérêt légitime de l'éditeur et nécessite le consentement ».

Ces affirmations devraient être nuancées :

- Premièrement, le RGPD ne créé pas de hiérarchie entre les bases légales prévues à l'article 6. Il ne précise pas non plus que le profilage devrait reposer « par principe » sur le consentement. En effet, aux termes de son article 22, le consentement n'est requis que dans le cas d'un profilage suivi d'une prise de décision entièrement automatisée produisant des effets juridiques sur une personne ou l'affectant de manière significative de façon similaire[32] ;

- Deuxièmement, le consentement est effectivement nécessaire pour la publicité personnalisée quand des traceurs stockés dans le terminal sont utilisés au sens de l'article 5(3) de la directive ePrivacy. Ce n'est pas nécessairement le cas, le profilage n'impliquant en effet pas toujours le recours à un traceur stocké dans le terminal.

[31] Ibid.
[32] Article 22 du RGPD https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=OJ:L:2016:119:FULL

Nous demandons à la CNIL de clarifier ce point dans la prochaine version en détaillant précisant dans quel(s) cas précis le consentement s'impose.

Enfin, il serait pertinent que le projet de recommandation n'associe pas systématiquement et continuellement publicité et profilage. La publicité en ligne n'implique pas forcément des opérations de profilage. C'est par ailleurs une activité économique légale et légitime qui ne devrait pas systématiquement être mentionnée de façon péjorative.

- Sur l'usage intempestif du qualificatif « intrusif »

Les « pratiques intrusives » ou « l'intrusivité » reviennent de façon récurrente tout au long du projet de recommandation. Ce sont des concepts subjectifs, étrangers à la réglementation applicable et qui sont très largement sujets à interprétation *a fortiori* quand ils ne sont pas ou peu caractérisés. C'est le cas du projet de recommandation qui ne spécifie pas les différents types de données collectées et le degré « d'intrusivité » auquel ils pourraient être associés.

Par ailleurs, ces concepts sont dans la plupart de cas associés avec des agissements des éditeurs des applications et absents quand il s'agit de descriptions des pratiques des fournisseurs d'OS, notamment lorsque ces derniers collectent des permissions faisant doublon avec le consentement collecté par des éditeurs.

- Sur l'absence de développement relatives aux techniques de protection de la vie privée

L'objectif des recommandations de la CNIL ne doit pas se limiter à préciser les obligations des parties et à imposer des qualifications juridiques hors contexte. La CNIL pourrait aider les différents acteurs à recourir à des techniques de protection des données personnelles leur permettant de traiter les données de façon responsable et de mener leur activité en toute confiance. Il est dès lors regrettable que le projet de recommandation ne consacre aucun développement à ce sujet et se borne à renvoyer à des guides sur les *Privacy Enhancing Technologies* produits par l'OCDE et l'autorité de protection des données britannique. Cela nous semble non seulement insuffisant mais aussi inadapté de la part d'un régulateur national d'encourager à se référer à des travaux extérieurs à l'Union européenne et de surcroît en langue anglaise.

Il serait par ailleurs intéressant que la CNIL et ses homologues européens lancent un chantier sur la définition de la donnée personnelle pour éclairer le marché sur les différentes techniques de pseudonymisation et de dé-identification et comment ces dernières permettent de réduire le risque de réidentification de l'individu. Nous attirons l'attention de la CNIL sur les récentes lois en matière de la protection des données personnelles introduites

par certains états des Etats-Unis reconnaissent des régimes spéciaux applicables au partage des données "désidentifiées" ("de-identified information"). Il s'agit d'une approche pratique qui reconnait la valeur protectrice de certaines techniques de pseudonymisation.

## Concernant les éditeurs d'applications

- Un socle d'obligations supplémentaires que les éditeurs d'applications ne seront pas en mesure de supporter et qui ne reposent pas sur le RGPD

Le projet de recommandation opère un tournant important en disposant que les éditeurs d'application seraient très largement responsables tout au long du « cycle de vie » de l'application. La CNIL met en place un régime où les éditeurs d'applications vont devoir répondre à de nombreuses nouvelles obligations entrainant de nombreuses difficultés techniques et contractuelles pour un coût démesuré, notamment pour les plus petits d'entre eux[33].

Sur l'obligation d'auditer l'ensemble des SDK utilisés par les éditeurs

Cette obligation nous apparait non justifiée légalement, impossible techniquement et contractuellement et largement déséquilibrée.

A titre liminaire, il est important de noter qu'aucun article du RGPD ne prévoit une obligation générale d'audit a priori de l'ensemble des partenaires SDK. Le processus d'audit est utilisé par les éditeurs d'applications quand ces derniers estiment qu'il y a un besoin précis. Le RGPD prévoit bien la capacité pour le responsable de traitement de mener des audits de ses sous-traitants[34] mais en aucun cas une obligation générale d'audit global et a priori. La CNIL ne peut donc en l'espèce créer une obligation juridique de cette nature sans outrepasser le mandat qui lui est confié par la loi.

De plus, il est impossible dans les faits pour un éditeur d'applications d'auditer l'ensemble de ces SDK, *a fortiori* dès que ces derniers procèdent à un changement de quelconque nature, et ce pour deux principales raisons.

- **La première est qu'aucun éditeur n'a ni les ressources ni les compétences techniques à disposition pour procéder à ce type d'efforts particulièrement fastidieux**. Si les éditeurs avaient les compétences techniques, ils ne feraient pas appel à des

[33] Pour rappel, on compte près de 3,5 millions d'applications sur le Google Play et près de 2 millions sur l'Apple Store. Source Statista : octobre 2022, https://fr.statista.com/statistiques/571454/nombre-d-applications-disponibles-sur-les-principaux-app-stores/ .
[34] Article 28 RGPD https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=OJ:L:2016:119:FULL

développeurs pour les conseiller et n'utiliseraient pas de fournisseurs de SDK externes. Il n'est donc pas adapté d'imposer à des éditeurs d'applications d'avoir des compétences spécifiques pour auditer la gestion d'un SDK qu'ils utilisent justement parce qu'ils en sont dépourvus. Par ailleurs, il n'existe pas d'outil disponible sur le marché pour systématiser les audits. La fonctionnalité OWASP mentionnée par le projet de recommandation de la CNIL est un ensemble de bonnes pratiques permettant de sécuriser des applicatifs. Elle n'est pas pertinente pour répondre aux enjeux de protection des données personnelles présent dans ledit projet et s'applique plus spécifiquement aux applicatifs présents sur le web.

- La seconde relève du fonctionnement du marché mobile. **L'éditeur d'application n'est pas nécessairement en mesure de choisir les fournisseurs de SDK dans son application et ne dispose pas non plus de contrats avec chacun d'entre eux**. Cela relève de champ technique qui sont souvent laissés aux développeurs. Par ailleurs, le rapport de force n'est pas favorable à l'éditeur d'applications en l'espèce : beaucoup refuseront de se faire auditer pour des questions de secret des affaires ou d'absence d'engagement contractuel. Par ailleurs, la situation quant à l'utilisation des SDK repose sur les mêmes déséquilibres concurrentiels : les SDK des grandes plateformes sont dominants et quasi inévitables [35] et leur utilisation se fait dans des conditions d'application strictes et sur lesquelles les éditeurs n'ont aucune marge de manœuvre[36]. Il est donc strictement impossible qu'ils soient en capacité de les auditer.

Enfin, cette obligation nous apparait déséquilibrée. Tout d'abord parce qu'elle fait reposer l'intégralité de la charge sur un seul acteur de façon disproportionnée et n'intègre même pas une notion d'obligation de moyen ou de « meilleurs efforts » à l'inverse de ce qui a pu être décidé par la CNIL dans le cadre des cookies et autres traceurs[37]. Ensuite parce qu'elle ne protège pas du tout les éditeurs d'applications. A titre d'exemple, page 53 « *Dans les cas où les SDK sélectionnés affirment qu'ils permettent de collecter le consentement de manière licite, cette obligation devrait être formulée contractuellement et son respect audité* [38] » : le développeur ou l'éditeur doit réaliser l'audit mais on ne sait pas quelles seront les conséquences en cas d'infraction du SDK. Est-ce un motif de résiliation du contrat pour l'éditeur ? Si oui, dans quelles conditions ? Que se passe-t-il si le fournisseur de SDK est basé aux USA ? Est-ce que l'éditeur est en droit à demander une compensation financière de la part de SDK ? Comment calculer des éventuels dommages et intérêts surtout pour un éditeur

[35] Les SDK de Google, Apple et Meta sont installés sur respectivement 82%, 51% et 41% des applications mobiles disponible en France. Voir taux de pénétration des kits de développement logiciel (SDK) parmi les applications mobiles disponibles en France en janvier 2019 https://fr.statista.com/statistiques/966785/editeurs-logiciels-sdk-populaires- france/

[36] Voir les guidelines d'Apple qui définissent les conditions générales régissant l'utilisation des outils de développement Xcode et des SDK https://developer.apple.com/support/terms/

[37] Délibération de la formation restreinte n°SAN-2021-013 du 27 juillet 2021 concernant la SOCIETE x https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000043867129

[38] P. 53 du projet de recommandation

d'une nouvelle application ayant supporté les frais de développement mais n'ayant pas encore de chiffre d'affaires ?

Sur l'obligation de tenir à jour un registre des traitements

Le registre des traitements tel que présenté dans le projet de recommandation nous apparait aller, à nouveau, plus loin que le « registre des activités de traitement » prévu à l'article 30.1 du RGPD. D´autant plus que le « registre des activités de traitement » applicable aux sous-traitants, prévu à l'article 30.2 du RGPD, est bien limité aux catégories d'activités de traitement effectuées pour le compte du responsable du traitement. La CNIL ne peut imposer aux acteurs de mettre en place un registre de l'ensemble des traitements au nom du principe de redevabilité des acteurs comme cela est indiqué dans le projet de recommandation.

Par ailleurs, tenir un registre « traitement par traitement » est possible conceptuellement mais impossible en pratique. Cela imposerait de lister l'ensemble des SDK utilisés, des tiers concernés et/ou l'ensemble des prestataires, par exemple dans le cadre de l'utilisation d'une CMP TCF. L'exécution de cette démarche de manière fiable s'avère difficile, car elle dépend de plusieurs intervenants : les traitements sont mis en œuvre par les éditeurs d'applications, les autorisations sont gérées au niveau de chaque application, les fournisseurs de SDK accèdent aux données traitées uniquement lorsqu'ils sont intégrés à une application. Cependant, les données auxquelles les SDK ont accès peuvent varier sans que les éditeurs ne soient toujours informés, ce qui rend complexe toute tentative de prédiction « traitement par traitement » pour un éditeur d'applications.

Le projet de recommandation mobile ne devrait pas entériner des différences de pratiques de mises en conformité selon l'environnement donné. En l'occurrence l'environnement web prévoit la tenue d'un registre de traitement mis à la charge des sous-traitants par l´article 30.2 qui ne doit pas recenser et analyser l'intégralité des traitements de données personnelles mis en œuvre.

Il est important que la CNIL comprenne que s'assurer de la conformité du traitement représente un coût technique et financier élevé, *a fortiori* si les dispositions légales sont différentes selon les environnements.

Sur les dispositions relatives aux politiques de confidentialité

Le projet de recommandation contraint les éditeurs d'applications à présenter leur politique de confidentialité « avant tout lancement ou téléchargement de l'application[39] ». Si cela correspond à la pratique de façon générale (notamment sur demande des fournisseurs de

[39] Page 33 du projet de recommandation

magasins d'applications), il apparait que cette obligation ne repose sur aucune base légale réelle puisque les éditeurs d'applications n'ont l'obligation que de la présenter au moment de la collecte.

Par ailleurs, pour ce qui est de la présentation des politiques de confidentialité, le rôle du régulateur n'est pas de s'immiscer dans leurs choix éditoriaux et de conception. Il s'agit de s'assurer que la politique de confidentialité est suffisamment lisible et compréhensible pour permettre un consentement informé et éclairé des utilisateurs. Pour le reste, que ce soit la présentation, la police utilisée ou encore la présence « d'éléments visuels » ou non, c'est à l'éditeur applications de choisir les éléments qui sont adaptés et d'utiliser les moyens à sa disposition pour le faire.

Nous souhaiterions que la CNIL clarifie ici cette position et relève qu'il ne s'agit que de recommandations et non d'une obligation supplémentaire.

Sur l'exercice des droits

Le projet recommande de « mettre à disposition des personnes un centre de gestion des droits au sein de l'application où l'ensemble des droits peuvent être exercés [40]». Ce n'est qu'une recommandation puisqu'ils n'existe en effet aucun moyen privilégié dans les textes pour répondre à l'exercice des droits, comme indiqué plus haut. Cependant, la suite du texte prête à confusion puisqu'il est mentionné que « l'éditeur doit demander à son développeur de le conseiller dans cette démarche [41] », donnant l'impression qu'il s'agit en réalité d'une obligation.

Dans la droite ligne de notre remarque générale sur la confusion entre obligations et recommandations, il s'agirait de reformuler cette partie et de n'indiquer seulement que, lorsqu'il estime ce moyen pertinent pour répondre à l'exercice des droits, l'éditeur d'applications peut s'appuyer sur les compétences du développeur pour le mettre en œuvre.

- Des inquiétudes sur le recueil du consentement

Sur la désintermédiation croissante des éditeurs d'applications et de leurs utilisateurs

Le projet de recommandation relatif aux applications mobile risque de renforcer la désintermédiation forcée des éditeurs d'applications dans la gestion des permissions et le recueil du consentement de leurs utilisateurs et clients.

[40] P. 34 du projet de recommandation
[41] Ibid.

Nous craignons que le projet de recommandation ouvre la voie à une gestion prépondérante du système d'exploitation dans le recueil du consentement des utilisateurs. La CNIL recommande tout au long dudit projet aux éditeurs d'analyser d'abord les permissions obtenues ou non et de choisir ensuite s'il y a besoin d'une CMP. Ce basculement emporte des conséquences économiques et pratiques très importantes pour les éditeurs d'applications, comme déjà relevées par l'Autorité de la concurrence concernant l'article 10 du projet de règlement ePrivacy sur le consentement au niveau du navigateur[42].

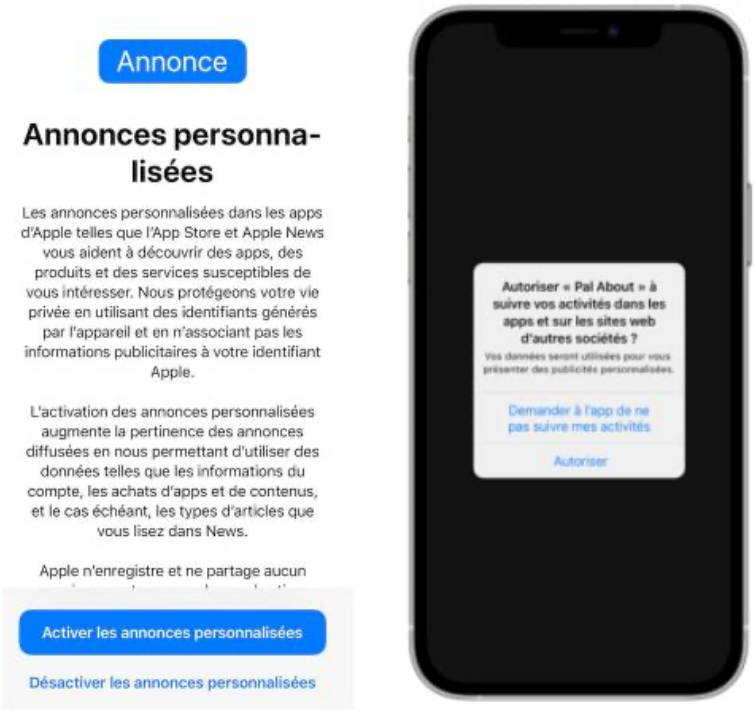
Tout d'abord, l'exemple de l'introduction d'Apple ATT nous a démontré que la désintermédiation de la gestion du recueil du consentement préalable entraine des conséquences financières majeures. Ainsi, on estime à 16 milliards de dollars les pertes causées sur les éditeurs d'applications du fait de l'introduction d'Apple ATT 2022[43]. Elles sont principalement la conséquence de l'introduction d'une fenêtre très peu personnalisable, anxiogène, redondante et uniquement appliquée aux applications tierces. Aujourd'hui, les éditeurs d'applications obtiennent des taux de consentement de l'ordre de 75-85% lorsqu'ils gèrent leurs propres CMP alors que cela tombe à 25-35% avec la fenêtre Apple ATT.

Par ailleurs, le fournisseur du système d'exploitation a déjà en partie forcé la désintermédiation des éditeurs d'applications vis-à-vis de leurs utilisateurs. Un éditeur est dépendant du fournisseur de l'OS pour obtenir des données et pour l'utilisation de l'ensemble des permissions dont il a besoin (push notification, géolocalisation, accès aux contacts etc.). Cela pourrait et devrait être organisé dans l'autre sens. A tout le moins, le régulateur de la protection des données devrait demander aux fournisseurs d'OS de prévoir cette possibilité et en clarifier les modalités concrètes dans la prochaine version de la recommandation.

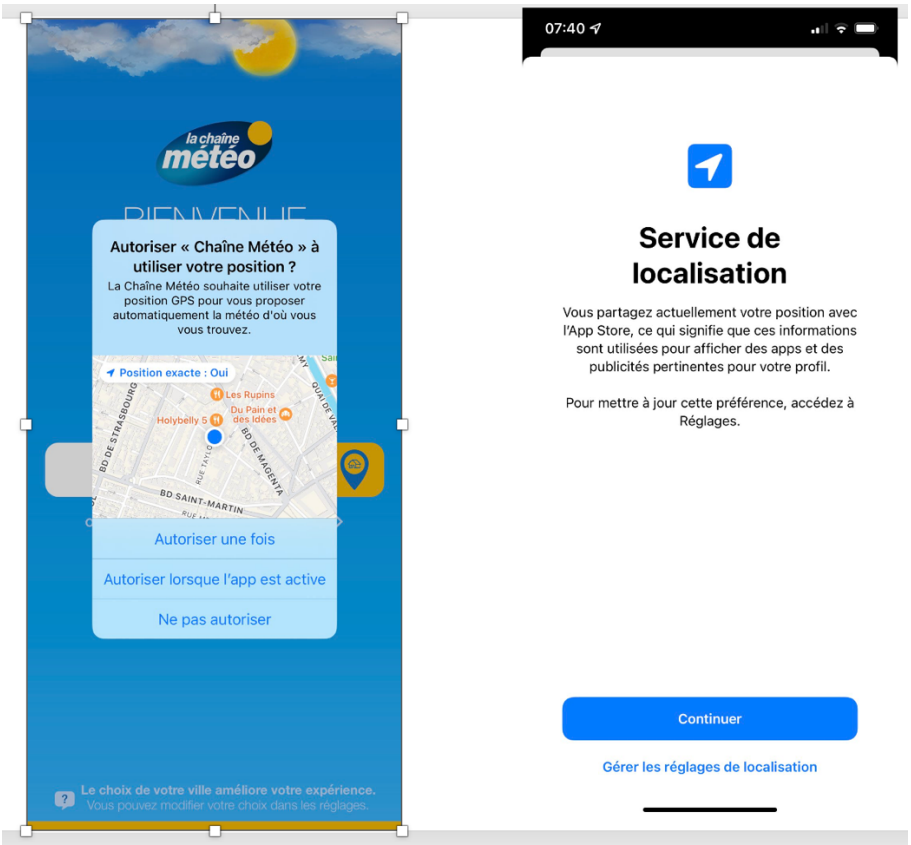
C'est d'autant plus important que cette mainmise croissante sur le recueil du consentement pourrait être utilisée à des fins anticoncurrentielles comme cela se manifeste déjà sur l'environnement iOS, voir exemples ci-dessous :

[42] Avis n° 18-A-03 du 6 mars 2018 portant sur l'exploitation des données dans le secteur de la publicité sur internet https://www.autoritedelaconcurrence.fr/sites/default/files/commitments/18a03.pdf

[43] Cabinet Lotame, 2022 : https://www.lotame.com/idfa-and-big-tech-impact-one-year-later/




Exemple du recueil du consentement pour les activités publicitaires d'Apple à gauche et d'ATT pour les tiers à droite




Exemple de permission pour une application tierce à gauche et pour l'App Store à droite.

Nous demandons à la CNIL de ne pas aggraver la désintermédiation des éditeurs d'applications avec les utilisateurs et de considérer qu'une autre voie est techniquement et légalement possible.

Sur la mise en danger du marché des CMP

La possibilité laissée aux fournisseurs de systèmes d'exploitation de gérer le consentement risque de déstabiliser fortement le marché des CMP et l'ensemble des expertises qui se sont développées depuis plusieurs années. Cela signifie que près de 75% du trafic Internet en France[44] pourrait ne plus être accessible aux dizaines d'entreprises fournisseurs de CMP, y compris de nombreuses entreprises françaises et européennes. Le projet de recommandation risque, en l'état actuel de la rédaction, d'entraver fortement le développement de beaucoup d'entreprises de CMP et de mettre en danger la santé économique de tout un marché.

Par ailleurs, cela emporte des conséquences directes pour les éditeurs d'applications, autres que celles évoquées plus haut :

- L'impossibilité de faire jouer la concurrence entre les différents fournisseurs de CMP et de bénéficier de leurs expertises multiples et conseils stratégiques pour la gestion de leurs applications. Les fournisseurs d'OS, acteurs globaux par essence, ne pourront jamais bénéficier de l'expertise et de la connaissance des spécificités locales des fournisseurs de CMP ;

- Une perte nette de pouvoir de négociation puisque les éditeurs d'applications n'exerceront aucune influence sur les modalités des permissions, la façon dont elles vont être définies, le texte associé aux finalités etc. et devront adopter une approche « *one size fits all* » ne prenant pas en compte leurs spécificités (diversité des applications, taille, type de marché, etc.) ;

- Une perte d'influence de la marque avec l'obligation de créer deux expériences distinctes pour l'utilisateur selon le terminal utilisé (web ou mobile). Par exemple, l'identité de marque ne pourrait plus être affichée sur les fenêtres des fournisseurs d'OS qui seraient nécessairement non personnalisées ;

- Manque de cohérence entre la description des finalités poursuivi par un même service sur web, iOS et Android entrainant une possible confusion des utilisateurs concernés sur les traitements des données personnelles entrepris par les applications qu'ils utilisent ;

[44] Source Médiamétrie, 2022.

- Un risque de fraude plus important du fait de la différence d'environnement selon les terminaux.

Nous demandons à la CNIL de revoir ces points à l'aune des éléments ci-dessus et sur la base de la nécessaire neutralité concurrentielle du projet de recommandation.

- Vers un renforcement des relations asymétriques avec les fournisseurs de magasins d'applications et de systèmes d'exploitation

<u>Sur l'identifiant publicitaire</u>

Dans son projet de recommandation, la CNIL valide la pratique consistant à ce que seuls les fournisseurs de systèmes d'exploitation puissent être en mesure de fournir des identifiants publicitaires. Ce n'est pas parce qu'il s'agit de la manière dont a principalement fonctionné le marché depuis plusieurs années avec notamment les identifiants publicitaires mobiles de Google (GAAID) et d'Apple (IDFA) que les éditeurs d'applications en capacité d'en développer devraient en être empêchés. Ainsi, la CNIL pourrait tout à fait exprimer la possibilité pour les éditeurs d'application de produire des identifiants publicitaires propres et d'en tracer les limites d'utilisation.

Cela nous apparait également problématique d'un point de vue concurrentiel car cela renforce la dépendance des tiers aux fournisseurs de systèmes d'exploitation dans un contexte où :

- Les environnements logués qui dominent le marché publicitaire comme celui d'Apple n'ont pas besoin de ces identifiants publicitaires pour fonctionner de façon efficace ;

- la restriction et/ou la suppression du partage des identifiants publicitaires mobiles types IDFA ou GAAID (Apple ATT et Privacy Sandbox) témoigne du pouvoir de marché de ces mêmes acteurs via leur capacité d'entraver la collecte de données des tiers et donc d'entraver leur modèle économique des tiers, souvent au profit de leurs propres services.

Enfin, à l'aune de la lecture de l'ensemble du document et de l'analyse du partage des responsabilité sur la chaîne de valeur, nous ne comprenons pas pourquoi un système d'exploitation comme iOS ne serait pas responsable de traitement conjoint avec l'éditeur d'applications pour la mise à disposition de l'identifiant publicitaire.

Sur la justification de création de compte

Le projet de recommandation émet un nouveau principe général -dont on ne sait d'ailleurs pas s'il s'agit d'une recommandation ou d'une obligation et le cas échant la base légale sur laquelle est serait fondée- qui ne devrait pas, selon notre analyse, figurer dans ce type de document. Il est indiqué en effet que « l'éditeur ne devrait imposer la création d'un compte que si cela est nécessaire, et envisager des alternatives pour éviter de collecter adresses de courriel et mots de passe[45] ». De cette façon, la CNIL se substitue à nouveau au législateur et instaure une règle selon laquelle la création de compte, lorsque qu'elle n'est pas « nécessaire », serait illégale. Le projet de recommandation devrait plutôt s'attacher à indiquer aux éditeurs d'applications quelles sont limites de la création de compte et quelles conditions les éditeurs d'applications devraient respecter pour être conforme à la réglementation applicable.

Par ailleurs, ce principe général pose trois problématiques principales :

- La première est celle relative à ce qui est de l'ordre du nécessaire et ce qui de l'ordre de l'optionnel. La CNIL ne précise pas ce qu'elle entend à ce sujet laissant les éditeurs d'applications dans le flou ;

- La seconde relève de l'incohérence avec d'autres obligations imposées aux éditeurs d'applications notamment de celles de modération ou de protection des mineurs pour lesquelles il est très compliqué d'y répondre de façon satisfaisante sans identifier les utilisateurs via la création de compte. Cette recommandation/obligation est donc inadaptée à l'état actuel du droit ;

- Enfin, la dernière est d'ordre concurrentiel. Le projet de recommandation souhaite restreindre la possibilité pour les éditeurs de connaitre leurs clients alors même qu'ils sont en concurrence avec des *walled-gardens* qui ont adopté une logique de login cross-device unifié. Cette recommandation/obligation pourrait ainsi renforcer le déséquilibre entre les grands acteurs d'un côté et le reste de l'autre.

Enfin, nous tenions à signaler que la CNIL a récemment interrompu son projet de position relative à l'obligation de créer un compte utilisateur pour effectuer un achat en ligne dans l'attente des discussions au sein de l'EDPB et « afin d'établir une position harmonisée et d'assurer une application uniforme de la réglementation [46]».

[45] P. 30 du projet de recommandation
[46] https://www.contexte.com/actualite/numerique/les-cnil-europeennes-reflechissent-a-un-mode-invite-obligatoire-pour-les-sites-de-vente-en-ligne_174594.html

Pour toutes ces raisons, nous estimons que ce point devrait être retiré de la prochaine version de la recommandation.

- Autres commentaires

Sur le tableau des « permissions et protection des données dès la conception »

Le projet de recommandation s'adonne ici à une synthèse de tous les textes pour accompagner les acteurs quant à l'utilisation des permissions. Deux choses très importantes n'y figurent pas :

- Les exemptions dans le cadre de la directive ePrivacy ne sont pas mentionnées et la CNIL ne présente pas les différentes possibilités qui sont à disposition des éditeurs pour ne pas demander le consentement de l'utilisateur. De façon globale, le projet de recommandation n'apporte aucun progrès quant à ce qui peut être fait par un éditeur sans le consentement de l'éditeur, notamment liées à la fraude et à certains traitements spécifiquement nécessaires au service nécessitant la collecte de données personnelles [47];

- La relation entre le recueil du consentement et l'affichage de permissions n'est pas non plus explicitée ici.

## Concernant les développeurs d'applications

- Sur la difficile compréhension de l'articulation entre consentement et les permissions

Le projet de recommandation de la CNIL inclut les développeurs dans la participation à la mise en conformité « en matière d'usage de traceurs et de recueil du consentement » des éditeurs d'applications. Dans ce cadre, la CNIL explique les moyens pour les développeurs d'articuler consentement et permissions.

Les permissions sont gérées en pratique par les fournisseurs de systèmes d'exploitation. Elles correspondent à des demandes d'accès au terminal en fonction des déclarations des éditeurs d'applications que l'utilisateur peut accepter ou refuser. Le projet de recommandation ne mentionne pas les accès au terminal qui sont nécessaires pour le fonctionnement du service et pour lesquels l'éditeur d'applications est, sur le fondement de la directive ePrivacy, simplement tenu d'informer l'utilisateur et non de lui demander son accord. Cette possibilité

[47] Exemples :

devrait donc être intégrée dans le projet de recommandation au risque de voir les applications ne pas être en mesure de fonctionner. En outre, c'est une approche particulièrement inéquitable puisque les éditeurs d'applications tiers ne peuvent à date fournir un lien cliquable emmenant les utilisateurs directement vers les paramètres, contrairement aux applications natives et notamment celles d'Apple.

Le projet de recommandation indique que « dans ce cas, le consentement donné à travers la CMP consécutivement à un refus exprimé lors d'une demande de permission ne pourra être considéré comme univoque, et ne sera ainsi pas valable au titre de la réglementation[48] ». Il s'agit ici d'un changement de paradigme grave que nous demandons à la CNIL de retirer pour les raisons suivantes :

- La CNIL ne peut demander au développeur de faire prévaloir le choix d'un utilisateur à une permission à l'obtention d'un consentement valable au sens du RGPD et de la directive ePrivacy. Cela va à l'encontre de la réglementation applicable en rendant l'obtention d'un consentement valide inutile et également à l'encontre des règles de droit civil qui veulent qu'un consentement plus spécifique et plus récent prévale sur une permission plus générale et plus ancienne ;

- Cette approche semble en contradiction avec le RGPD qui définit les conditions requises pour la validité du consentement sous le contrôle de la Cour de Justice de l'Union européenne. Au contraire, la notion de permission n'a aucune existence juridique et pourrait donc être obtenue dans des conditions bien moins strictes que celles applicables au recueil du consentement ;

- Cela prive l'utilisateur de sa capacité et de sa liberté de choisir et entraine une situation préjudiciable pour ce dernier et l'éditeur d'applications. Il apparait en effet pernicieux que la CNIL recommande aux développeurs de **NE PAS** tenir compte du consentement légalement obtenu d'un utilisateur par un éditeur d'applications. Cela signifierait, dans une situation inverse, à savoir l'octroi de permission suivi d'un refus de consentement, que la règle de primauté de permission sur le consentement proposée par la CNIL autoriserait l'éditeur d'applications à ne pas respecter le refus de consentement de son utilisateur pour les traitements correspondant aux permissions ;

- Enfin, cela renforce le pouvoir de marché des fournisseurs de systèmes d'exploitation en faisant prévaloir les permissions qu'ils gèrent sur les consentements demandés directement par les éditeurs d'applications pour leurs services.

[48] P. 51 du projet de recommandation

Nous sommes ainsi particulièrement inquiets de voir que le projet de recommandation de la CNIL fait triompher les demandes de permission des fournisseurs de systèmes d'exploitation sur celles des autres. Il s'agit ici d'un problème concurrentiel majeur qui favorise à nouveau les fournisseurs de systèmes d'exploitation sans la moindre responsabilité supplémentaire et qui renforce le déséquilibre entre le fonctionnement d'un même service sur le web et sur l'environnement mobile.

- Clarification de la responsabilité entre le développeur et l'éditeur d'application

L'intérêt du projet de recommandation pourrait être de clarifier les responsabilités de chacun selon une situation donnée. Il faudrait pour cela que la CNIL accepte d'en tracer les limites selon les différents acteurs en présence.

Lorsqu'il est indiqué que le développeur « doit s'assurer que le responsable du traitement est informé des choix techniques opérés et de leurs implications, pour lesquels le développeur engage sa responsabilité contractuelle [49]» alors qu'il est mentionné plus haut que l'éditeur est responsable de la maîtrise technologique de ses applications, cela n'aide pas à savoir qui est responsable dans ce cas entre le développeur et l'éditeur d'applications.

Il faudrait davantage prendre en compte les réalités du terrain et ainsi tracer ls contours des responsabilités des acteurs : c'est le développeur qui devrait être responsable du développement et de la supervision technique de l'application car c'est lui qui dispose des compétences pour le faire contrairement à l'éditeur d'applications.

- Autres commentaires

<u>Sur la façon de recueillir le consentement sur mobile</u>

Le projet de recommandation indique aux développeurs comment aider les éditeurs d'applications à recueillir le consentement et présente trois interfaces différentes pour « permettre la lisibilité des fenêtres dans un environnement mobile[50] ». Aucun des visuels présentés ne reprend l'interface avec le « continuer sans accepter » pour permettre à l'utilisateur d'exprimer son refus au dépôt et à la lecture de traceurs, ce qui n'est pas cohérent avec la recommandation proposant des modalités pratiques de mise en conformité en cas de recours aux « cookies et autres traceurs[51] ». Comme indiqué précédemment, l'objectif de cette recommandation est d'apporter des réponses et, en l'espèce, elle soulève de nouvelles

[49] P. 48 du projet de recommandation
[50] P. 50, 51 du projet de recommandation.
[51] P. 10 Délibération n° 2020-092 du 17 septembre 2020 portant adoption d'une recommandation proposant des modalités pratiques de mise en conformité en cas de recours aux « cookies et autres traceurs » https://www.cnil.fr/sites/cnil/files/atoms/files/recommandation-cookies-et-autres-traceurs.pdf

questions. Nous demandons que la CNIL insère ce visuel pour assurer une cohérence globale avec le cadre applicable sur le web.

Par ailleurs, il est important de noter cette interface est largement présente sur le marché français et a nécessité un travail important et coûteux de la part de l'ensemble du marché.

Sur la non-transmission d'identifiant inter-applications à des fournisseurs de SDK

« La transmission d'identifiants inter-applications à des fournisseurs de SDK devrait être évitée[52] ». Nous considérons ce passage comme l'affirmation d'une position de principe de la CNIL et non comme une recommandation adressée aux fournisseurs de SDK.

A nouveau, le projet de recommandation relatif aux applications mobiles ne devrait pas être utilisé pour affirmer de nouveaux principes.

Nous souhaitons le retrait de ce point.

Sur l'usage de sécurisation du service

Il serait intéressant que la CNIL précise quels traceurs ou quel(s) type(s) de traceurs pourraient être utilisés pour « prévenir d'attaques en déni de service (…) ou de bourrage d'identifiants » comme retenu à la page 29 du projet de recommandation.

La sécurité est une obligation légale de responsable de traitement et de ses sous-traitants. Elle fait partie d'un niveau de service expressément demandé par l'utilisateur. Il nous semblerait utile d'affirmer l'existence de traceurs permettant la sécurité des applications et ne nécessitant pas le consentement préalable des utilisateurs.

## Concernant les fournisseurs de SDK

- Gestion du consentement et permissions

La partie dédiée à la conformité des fournisseurs de SDK en matière d'usage de traceurs et de recueil du consentement soulève plusieurs problématiques importantes :

- La première découle du fait que la CNIL ouvre clairement la voie pour les fournisseurs de systèmes d'exploitation de gérer l'obtention d'un consentement valable pour le reste de l'écosystème via des demandes de permission comme App Tracking

[52] P. 48 du projet de recommandation

Transparency (ATT). Compte-tenu du pouvoir de marché des fournisseurs de systèmes d'exploitation, de l'impact qui a été celui d'Apple ATT[53] sur l'ensemble de l'écosystème, de l'importance du marché des CMP ainsi que des nombreuses plaintes en cours en Europe dont en France[54], cette possibilité devrait être écartée ;

- La deuxième relève d'un défaut d'homogénéité et de cohérence avec des dispositions précédentes du projet de recommandation. Comme expliqué plus haut, la permission est jugée comme primant sur le consentement dans le cas des développeurs[55] alors qu'il est indiqué ici page 65 que les permissions sont insuffisantes pour recueillir le consentement de l'utilisateur ;

- Il n'est pas non plus fait mention des permissions nécessaires à l'exécution du service pour lequel l'utilisateur a téléchargé une application[56]. Dans l'état actuel du projet de recommandation et notamment au regard des dispositions supplémentaires concernant l'absence et la révocation, de nombreuses applications pourraient ne pas être en mesure de fonctionner, au détriment des utilisateurs finaux.

Nous recommandons ainsi à la CNIL de revoir cette partie à l'aune des éléments ci-dessus.

- Nouvelles obligations pour les fournisseurs de SDK

<u>Sur le registre des activités de traitement</u>

Le projet de recommandation revient sur le registre de traitement tenu par le fournisseur de SDK. Le document précise que le ce dernier doit tenir son propre registre des activités traitement qu'il soit sous-traitant ou responsable de traitement et ce sur la base de l'article 30 du RGPD. Ledit registre doit comporter l'ensemble des données collectées pour chaque traitement. Cela nous paraît être une surinterprétation de l'article 30.1 du RGPD qui emporte une quantité substantielle de détails supplémentaires à fournir, venant faire peser un poids important sur les fournisseurs de SDK.

De la même manière, le sous-traitant n'est pas tenu par l'article 30.2 du RGPD de détailler de façon spécifique l'ensemble des différents traitements au contraire de ce qui est indiqué dans le projet de recommandation. L'obligation pour les sous-traitants est d'ordre général, à savoir

[53] Voir question 6 de la réponse Alliance Digitale au questionnaire relatives aux enjeux économiques de la collecte de données mobiles.
[54] Voir la récente Notification de griefs de l'Autorité de la concurrence française, en date du 25 juillet 2023 : https://www.autoritedelaconcurrence.fr/fr/communiques-de-presse/publicite-sur-applications-mobiles-ios-le-rapporteur-general-indique-avoir
[55] Voir page 51 du projet de recommandation
[56] Voir la partie dédiée à l'articulation des permissions et du consentement pour le développeur

de tenir un registre comprenant « toutes les catégories d'activités de traitement effectuées pour le compte du responsable du traitement[57] ».

Il est par ailleurs matériellement impossible pour un sous-traitant de détailler pour chaque traitement, l'ensemble des données collectées. En l'espèce, un sous-traitant ne contrôle pas ce que les activités du client et n'est pas censé y avoir accès. Les traitements sont entre les mains du responsable de traitement.

Nous tenons à noter à nouveau que cette obligation supplémentaire renforce le déséquilibre créé par le projet de recommandation entre l'environnement web d'un côté et le mobile de l'autre.

Sur l'usage des traceurs

Il est indiqué que le « fournisseur de SDK doit informer précisément ses partenaires sur les traceurs utilisés qui mettent en œuvre des opérations de lecture et/ou écriture sur le terminal de l'utilisateur[58] ». Ces informations sont en pratique présentes sur les contrats signés par les fournisseurs de SDK avec leurs clients ainsi qu'au sein des *Consent management platforms*.

Cependant, le terme « partenaire » vient créer une confusion superflue, renforçant ainsi impression selon laquelle le projet de recommandation soulève davantage de questions qu'il n'en résout.

Il serait pertinent d'avoir une clarification du terme « partenaire » : s'agit-il des clients ? des fournisseurs CMP ? des utilisateurs ? Des partenaires ayant la qualification de sous-traitants ?

Sur la documentation des permissions

Le commentaire sur la confusion autour du terme « partenaire » s'applique aussi à cette partie.

Cette obligation est potentiellement très fastidieuse notamment pour les fournisseurs de SDK de mesure qui sont obligés de croiser les données de leurs clients pour s'assurer de la pertinence des services qu'ils proposent.

Nous souhaiterions obtenir des clarifications sur ce point dans la prochaine version du document.

[57] Article 30.2 RGPD https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=OJ:L:2016:119:FULL
[58] P. 62 du projet de recommandation

- Autres

Définition du fournisseur de SDK

Il est « défini comme l'entité personne morale qui met à disposition un ou plusieurs SDK destinés à être intégrés dans des applications mobiles[59] ». Nous tenons à alerter la CNIL sur ce point : le fournisseur de SDK n'est pas nécessairement une personne morale. Si l'on tient à cette définition, cela signifie soit que la CNIL force à la création d'entreprise, ce qui n'est pas son rôle, soit que les fournisseurs de SDK qui seraient des personnes physiques seraient exclus du périmètre de la recommandation.

Mise à jour obligatoire demandée par le fournisseur de systèmes d'exploitation

Le projet de recommandation donne la possibilité au fournisseur de système d'exploitation de demander au fournisseur de SDK de mettre à jour son service lorsqu'il existe des solutions « plus protectrices de la vie privée pour traiter certaines informations[60] ».

Nous ne pouvons comprendre cette immixtion du fournisseur d'OS dans la relation entre un éditeur d'applications et son fournisseur de SDK. Dans le cas d'espèce, c'est à l'éditeur d'échanger avec son SDK sur de potentielles solutions plus protectrices pour les utilisateurs et il n'est en aucun cas dans l'obligation de lui forcer une mise à jour tant que le service respecte la réglementation en vigueur. Il existe un environnement concurrentiel des fournisseurs de SDK, l'éditeur est en capacité de changer ses prestaires le cas échéant et n'a absolument pas besoin de l'intervention du fournisseur d'OS.

Par ailleurs, cela viendrait consacrer une position d'arbitre de ce dernier, en capacité donc d'arbitrer entre ce qui est très protecteur, ce qui est protecteur ou ce qui ne l'est pas. Les fournisseurs de systèmes d'exploitation n'ont pas vocation à endosser ce type de rôle au risque de renforcer encore plus leur position de gatekeeper au sens de l'article 3 du Règlement 2022/195 dit Digital Markets Act (DMA)[61].

Nous souhaitons ainsi le retrait de ce passage de la recommandation relative aux applications mobiles.

[59] P. 59
[60] P. 61 du projet de recommandation
[61] https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32022R1925

## Concernant les systèmes d'exploitation

- Une mainmise confirmée sur les permissions et croissance quant à la gestion du consentement

Le projet de recommandation consacre le fournisseur de systèmes d'exploitation comme l'un des acteurs principaux du recueil du consentement sur mobile et ce faisant, son rôle de gatekeeper sur le marché. Le document indique notamment que « les fenêtres de permission devraient directement permettre d'obtenir un consentement valable [62]» ouvrant clairement la voie à une gestion de l'obtention du consentement au sens de la réglementation applicable par les fournisseurs de systèmes d'exploitation.

Nous nous opposons en tout point à cette pratique qui va nécessairement avantager la situation des deux principaux et quasi uniques fournisseurs d'OS au détriment de l'ensemble des acteurs tiers. Nous rappelons que la mainmise du fournisseur d'OS sur les permissions n'est absolument pas une nécessité technique ou juridique. La gestion des permissions pourrait tout à fait être revenir aux éditeurs d'applications eux-mêmes puisqu'il s'agit de leur relation avec les utilisateurs et non celles des fournisseurs d'OS. Il est alarmant que la CNIL ne prévoie pas ce cas de figure et entérine une situation de marché anormale, puisque ne résultant que de la domination des deux principaux OS sur le reste de l'écosystème.

Au-delà des considérations d'ordre concurrentiel, nous nous attarderons ici sur les éléments qui soulèvent de nombreuses interrogations au sein de Alliance Digitale :

- Les permissions ne correspondent pas nécessairement à des situations dans lesquelles le consentement de l'utilisateur est requis. Il s'agit tout particulièrement d'une situation problématique sur iOS puisque les éditeurs d'applications ne peuvent indiquer à Apple que certaines permissions ne sont pas soumises légalement au consentement de l'utilisateur. Apple contraint ainsi les éditeurs à requérir l'accord de l'utilisateur sur certaines permissions alors même qu'ils n'y sont pas contraints par la réglementation applicable. Le projet de recommandation devrait traiter cet enjeu et forcer Apple à changer ses pratiques ;

- Par ailleurs, tous les traitements de données ne sont pas soumis à des permissions. Si la permission pourrait valoir consentement comme semble le projeter le projet de recommandation, cette permission se limite à une finalité propre à l'accès au terminal et ainsi aux seules exigences de la directive ePrivacy. Les éditeurs d'applications devront quand même afficher aux utilisateurs leur CMP propre qui couvre les finalités liées à la directive ePrivacy et au RGPD pour respecter leurs obligations légales. Il est

[62] P. 77 du projet de recommandation.

donc erroné d'indiquer que cette situation serait à même de « minimiser la fatigue du consentement [63]». Par ailleurs, d'autres solutions existent pour limiter la « fatigue du consentement », la première serait d'établir la possibilité d'un consentement cross-device pour l'ensemble des terminaux utilisés (web, mobile, télé connectée etc.).

Plutôt que de laisser les mains libres aux fournisseurs d'OS, nous invitons la CNIL à clarifier la relation entre d'un côté la permission et le consentement ePrivacy et la permission et le consentement RGPD de l'autre.

- Des dispositions contraires au *Digital Markets Act* qui renforcent leur position de marché

Plusieurs dispositions du projet de recommandation relatif aux applications mobiles ne tiennent pas compte de l'adoption du Règlement 2022/195 dit Digital Markets Act et de la désignation récente des services de plateformes essentiels des « gatekeepers [64] ». Plus spécifiquement elles semblent juridiquement contraires au texte, ce qui pourrait mettre en péril la pérennité légale dudit projet de la CNIL. Il en va de même pour certaines dispositions concernant les magasins d'applications sur lesquelles nous revenons plus bas.

Vous trouverez ci-dessous les dispositions du projet de recommandation qui apparaissent être en contradiction avec le DMA :

- Le fait d'empêcher « techniquement et/ou contractuellement les éditeurs d'applications d'accéder à certaines données[65] » est considéré par la CNIL comme une « mesure positive majeure pour préserver la vie privée des personnes[66] ». C'est une contradiction nette de la lettre et de l'esprit du DMA qui impose que le partage d'information se fasse dans l'autre sens afin de « *permettre un accès sans entraves et gratuit à ces données (…) et à cette fin un contrôleur d'accès ne devrait pas recourir à des restrictions contractuelles ou autres dans le but d'empêcher les entreprises utilisatrices d'accéder aux données pertinentes, et devrait permettre à ces entreprises d'obtenir le consentement de leurs utilisateurs finaux pour l'accès à ces données et leur extraction, lorsque ce consentement est requis en vertu du règlement (UE) 2016/679 et de la directive 2002/58/CE* [67] ». Certains articles du DMA contraignent plus spécifiquement les gatekeepers à fournir des données relatives aux effets d'une annonce publicitaire [68] ou des données agrégées et non agrégées sur les services

[63] Ibid.
[64] https://ec.europa.eu/commission/presscorner/detail/en/IP_23_4328
[65] P. 67 du projet de recommandation
[66] Ibid.
[67] Voir considérant 54 du DMA https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32022R0195
[68] Voir Article 5(g) et Considérant 53 du DMA.

fournis par les services de plateformes essentiels[69]. Les deux fournisseurs de systèmes d'exploitation i.e., Apple OS et Google Android étant tous les deux désignés comme services de plateformes essentiels, le fait d'empêcher techniquement ou contractuellement les tiers d'accéder à certaines données nous parait tout à fait contraire au DMA. Il s'agit dès lors d'un moment important pour la CNIL de redonner aux éditeurs d'applications la possibilité de gérer les permissions pour leurs propres services en toute conformité avec le droit applicable ;

- Le fait de recommander aux fournisseurs de systèmes d'exploitation « de refuser l'accès aux contacts en renvoyant une liste vide ou partielle de contacts, à la localisation en renvoyant des coordonnées aléatoires ou prédéfinies manuellement [70] » est inquiétant. Ce fonctionnement est prévu pour permettre à l'utilisateur de décliner une permission sans que l'éditeur d'application en ait la connaissance. Il s'agit d'un point **particulièrement problématique** puisqu'il autorise et recommande aux fournisseurs d'OS de produire des informations erronées aux éditeurs d'applications qui se fient pourtant aux contrôles qu'ils opèrent. Cette disposition est incompréhensible, va à l'encontre du DMA qui prévoit des sanctions en cas de fourniture d'informations inexactes par les gatekeepers ainsi qu'aux règles de droit civil et à la jurisprudence liée à la bonne foi dans l'exécution dans du contrat.

- Plus largement, il est important de mentionner que le Règlement 2022/68 dit Data Act empêche également les tiers de transférer les données qu'ils reçoivent à des entreprises désignées comme gatekeeper conformément à l'article 3 du DMA[71].

Nous demandons à la CNIL de revoir largement cette partie dédiée au rôle des fournisseurs de systèmes d'exploitation dans la conception et la gestion des systèmes de permissions.

- Autres

<u>Sur les systèmes de partage locaux mis à disposition par le fournisseur d'OS</u>

Le tableau récapitulatif dédié aux fournisseurs de systèmes d'exploitation établit la recommandation (ou l'obligation ?) de fournir des « systèmes de partages locaux inter-applications sont mis à disposition par l'OS [72] ».

[69] Voir Article 6.1 (i) du DMA
[70] P. 77 du projet de recommandation.
[71] Voir Article 6.2 (d) du Data Act : https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2022%3A68%3AFIN
[72] P. 84 du projet de recommandation, également p. 79

Aucune explication n'est donnée ici. Nous ne savons pas à quoi il est fait référence. Il serait donc utile que la CNIL nous aide à y voir plus clair et nous expliquer ce à quoi cela fait référence et pourquoi elle semble en recommander (ou obliger ?) sa mise à disposition par les fournisseurs de systèmes d'exploitation.

Nous rappelons là encore qu'une recommandation doit être claire et limpide pour ne pas soulever de questions supplémentaires de la part des acteurs concernés.

Sur les mises à jour de sécurité

Le projet de recommandation consacre une recommandation selon laquelle les fournisseurs de systèmes d'exploitation devraient « proposer systématiquement des mises à jour de sécurité de l'OS au moins jusqu'à 5 ans après l'achat du terminal ». Une fois cette durée échue, s'il existe des règles, le fournisseur d'OS devrait orienter l'utilisateur « vers des OS alternatifs qui supportent son terminal [73]».

Il serait intéressant de comprendre d'où provient cette durée de limitation et sur la base de quelle évaluation la CNIL recommande aux fournisseurs de systèmes d'exploitation de l'appliquer.

Par ailleurs, et comme relevé à plusieurs reprises dans notre réponse, l'utilisation de systèmes d'exploitation alternatifs est soi largement surestimé (exemple d'Android) ou tout simplement impossible (Apple iOS). Cette disposition apparait donc largement illusoire.

Sur l'outil de contrôle parental

Le projet de recommandation prévoit la mise en œuvre d'un outil de contrôle parental destiné à informer les éditeurs d'applications lorsqu'il s'agit d'un mineur. Ce point soulève des interrogations :

- Qu'est-ce que la CNIL entend par « utilisateur mineur » ? S'agit-il de la définition de mineur du RGPD en l'espèce 15 ans en France ou celle du code civil donc 18 ans ? Dans ce cas, l'individu entre 15 et 18 ans serait privé de sa liberté de consentir ou non à la publicité personnalisée ;

- Les éditeurs d'applications ont aussi des informations quant à leurs utilisateurs qui peuvent, par exemple, déclarer leur âge. En cas de conflit, quelles informations sont censées prévaloir ? Celles de l'éditeur d'application ou du fournisseur d'OS ?

[73] P. 80 du projet de recommandation.

Nous demandons à la CNIL de bien vouloir clarifier l'ensemble de ces points dans la prochaine version de sa recommandation.

## Concernant les magasins d'applications

- Un renforcement net de leur position de monopole

Sur leur rôle conseil aux éditeurs d'applications

Le projet de recommandation donne aux magasins d'applications un rôle de « conseils sur la mise en conformité avec les règles européennes de protection des données[74] » à destination des éditeurs.

Le magasin d'applications n'a pas à prodiguer des conseils quant à la conformité des éditeurs a fortiori sans porter aucune responsabilité juridique. C'est également dangereux puisque le fournisseur de magasin d'applications, déjà en position dominante et disposant d'applications propre en concurrence avec le reste de l'écosystème applicatif, pourrait tout à fait utiliser cette position à des fins anticoncurrentielles.

Par ailleurs, comme indiqué dans les remarques générales, nous pensons qu'il n'est pas à la CNIL de définir les contours juridiques du devoir juridique mais au juge civil.

Nous souhaiterions le retrait de ce point.

Sur l'information quant au financement

Il est indiqué que des informations quant au financement des applications pourraient être affichées dans les pages de chaque application au sein des magasin. Nous percevons cette recommandation comme un élément superflu et potentiellement dangereux.

Superflu car ces informations sont déjà accessibles aux utilisateurs dans les CMP des éditeurs d'applications.

Dangereux tout d'abord car les éditeurs d'applications ne maitriseraient plus le message affiché aux utilisateurs et par conséquent n'aurait aucune garantie qu'il soit neutre et contextualisé. En outre, les éditeurs d'applications n'exerceraient plus aucune influence sur les critères de revue de ce type de messages. Ensuite parce que cela créé un énième avantage concurrentiel, les magasins d'applications restant maitres du message et des critères pour

[74] P. 87 du projet de recommandation

leurs applications natives. Enfin, cela nous semble être un blanc-seing pour imposer de nouvelles demandes d'informations dans le futur.

Nous demandons donc à la CNIL de supprimer cette recommandation.

Sur le score relatif à des critères et de vie privée et au mécanisme de signalement

La mise en exergue de la possibilité pour les magasins d'applications de mettre en place un « score relatif à des critères de vie privée [75] » qui pourraient être influencés par les signalements des utilisateurs nous apparait problématiques.

Tout d'abord, le projet de recommandation occulte à nouveau la position de marché occupée par les magasins d'applications et l'intérêt économique qu'ils pourraient avoir à administrer ce type d'outil. Il est important de rappeler que ces derniers ne sont absolument pas neutres et développent leurs propres applications, en concurrence avec l'ensemble du marché. Bien que le projet de recommandation insiste pour que la méthodologie soit déterminée de façon « transparente », le risque est grand de voir un acteur comme Apple profiter de cet outil pour favoriser ses propres services et ce, sans qu'aucune des parties prenantes ne puisse réellement s'y opposer. A ce titre, nous vous renvoyons au rapport commun de l'ICO et de la CMA qui s'inquiétaient de voir les questions de protection des données personnelles utilisées par certains acteurs comme instrument pour imposer leur vision et restreindre le développement de leurs concurrents (« privacy washing »)[76].

Deuxièmement, il est difficile de comprendre l'opportunité et l'utilité de l'introduction de tels dispositif par la CNIL, parallèlement à celui prévu à l'article 14 du Règlement 2022/2065 dit Digital Services Act[77]. Cet article établit une procédure normalisée, commune à l'ensemble des Etats-membres de l'Union européenne et qui présente des garanties importantes pour l'ensemble des parties prenantes concernées et pour les utilisateurs. Le mécanisme de signalement prévu par le projet de recommandation viendrait inutilement se juxtaposer à celui prévu par la loi, au détriment de l'ensemble des acteurs et tout particulièrement des utilisateurs qui ne seraient pas en mesure de comprendre la différence entre les deux mécanismes.

Enfin, ces dispositifs prévus par le projet de recommandation restent très largement opaques et soulèvent de nombreuses questions et inquiétudes : le score tiendra-t-il compte du contexte de l'application ? Sur quelle base le signalement des utilisateurs pourrait-il affecter ce score ? Qui traitera les signalements ? Une procédure de contestation sera-t-elle prévue ?

[75] P. 89 du projet de recommandation
[76] Information Commissioner's Opinion (ICO), Data protection and privacy expectations for online advertising proposals, 2021 https://ico.org.uk/media/about-the-ico/documents/4019050/opinion-on-data-protection-and-privacy- expectations-for-online-advertising-proposals.pdf
[77] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32022R2065

Et si oui de quel type et devant quel acteur ou quelle autorité ? Quelle place pour le régulateur et quel rôle pour le juge ? Des mécanismes de protection contre des attaques de concurrents sont-ils prévus (*take-down mechanisms*) ? Quelles sont les conséquences d'un score bas dans la présence et le référencement au sein du magasin d'applications ? Quelle articulation avec la procédure prévue par le DSA ? Y aura-t-il un bouton de signalement supplémentaire ? Comment distinguer les deux en tant qu'utilisateur ?

Au regard de ces éléments, nous recommandons à la CNIL de retirer ces dispositions de la prochaine version de la recommandation relative aux applications mobiles.

Sur la fourniture d'un point de contact pour les utilisateurs de l'UE

Le projet de recommandation demande que les magasins d'applications puissent s'assurer que les éditeurs d'applications aient un point de contact pour les utilisateurs de l'Union européenne souhaitant exercer leurs droits.

Il est à noter que le RGPD ne stipule pas explicitement la nécessité d'un point de contact physique pour traiter ces demandes, bien qu'il soit nécessaire d'apporter une réponse aux utilisateurs. Ce point nous semble par ailleurs contradictoire avec les recommandations de la CNIL qui encouragent les acteurs à utiliser des méthodes automatisées pour répondre aux demandes des utilisateurs.

- Des dispositions contraires au *Digital Markets Act*

Nous sommes inquiets de voir d'autres dispositions relatives aux magasins d'applications enfreindre le Digital Markets Act, à l'image de ce que nous avons exposé plus haut concernant les fournisseurs de systèmes d'exploitation.

Plusieurs dispositions nous apparaissent être en contradiction directe avec le DMA en recommandant explicitement aux magasins d'applications :

- D'obtenir toute une série de données provenant des éditeurs d'applications, y compris les catégories de données collectées, les tiers ayant accès à ces données ou encore la liste des systèmes de permission demandés par l'application[78]. Cela donne de surcroît un pouvoir de marché inestimable aux magasins d'applications en capacité d'avoir une visibilité importante sur l'activité de l'ensemble des éditeurs d'applications présents ;

[78] P. 86 du projet de recommandation

- D’exercer une influence sur le référencement des applications au sein de leurs magasin, notamment via la gestion du « score relatif à des critères de vie privée » tel que défini à la page 89 du projet de recommandation ;

- De demander à l’éditeur d’application de lui partager des informations liées à la protection des données comme les « finalités poursuivies, données traitées, modalités d’exercice des droits, durées de conservation » ;

- D’obliger les éditeurs d’applications à leur fournir leur documentation préexistante, y compris des informations protégées et ce, « afin d’encourager les bonnes pratiques en termes de protection des données ». C’est un détournement grave des fonctions des magasins d’applications qui s’opère, en outre, sans l’octroi d’une quelconque responsabilité supplémentaire pour ces derniers.

Nous demandons à la CNIL de prendre en compte l’adoption du Digital Market Act, la récente désignation des gatekeepers par la Commission européenne qui consacrent les magasins d’applications de Google et d’Apple en tant que services essentiels et ainsi de retirer l’ensemble des dispositions ci-dessus.