

Délibération n° 2020-137 du 17 décembre 2020 portant avis dans le cadre de la plainte déposée par certaines associations professionnelles de la publicité en ligne à l'encontre de la société Apple Inc. devant l'autorité de la concurrence

(demande d'avis n° 20019591)

La Commission nationale de l'informatique et des libertés,

Saisie par le rapporteur général de l'Autorité de la concurrence d'une demande d'avis concernant dans le cadre de la plainte de certaines associations professionnelles de la publicité en ligne à l'encontre de la société Apple Inc. devant l'autorité de la concurrence ;

Vu la convention n° 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

Vu le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE ;

Vu la directive 2002/58/CE du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques modifiée par la directive 2009/136/CE du 25 novembre 2009 ;

Vu le code de commerce, notamment son article R. 463-9 ;

Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, notamment ses articles 8-I-2° et 8-I-4°c ;

Vu le décret n° 2019-536 du 29 mai 2019 modifié pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ;

Vu la délibération n° 2020-091 du 17 septembre 2020 portant adoption de lignes directrices relatives à l'application de l'article 82 de la loi du 6 janvier 1978 modifiée aux opérations de lecture et écriture dans le terminal d'un utilisateur (notamment aux « cookies et autres traceurs ») et abrogeant la délibération n° 2019-093 du 4 juillet 2019 ;

Vu la 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 ».

Emet l'avis suivant :

L'Autorité de la concurrence (ADLC) a été saisie d'une plainte déposée le 23 octobre 2020 par plusieurs associations professionnelles de la publicité en ligne (ci-après « les associations requérantes ») à l'encontre de la société Apple Inc. et visant à obtenir la condamnation de la société sur le fondement des articles L. 420-2 du Code de commerce et 102 du Traité sur le fonctionnement de l'Union européenne, en raison de pratiques mises en œuvre par la société que les associations requérantes considèrent

comme anti-concurrentielles. Cette saisine est accompagnée d'une demande de mesures conservatoires.

Pour rappel, la société Apple a annoncé en juin dernier, qu'à partir d'iOS 14, les éditeurs d'applications souhaitant tracer leurs utilisateurs à des fins publicitaires (notamment en accédant à l'identifiant publicitaire des terminaux) ou permettre à leurs partenaires de le faire devront obtenir l'autorisation explicite de l'utilisateur par le biais d'une fenêtre « pop-up » conçue par la société Apple, dont une partie de l'architecture ne peut être modifiée (annexe 1). C'est cette pratique que les associations requérantes considèrent comme constituant un abus de position dominante.

Dans le cadre de l'instruction de cette plainte, l'ADLC a sollicité les observations de la Commission sur les questions en matière de protection des données à caractère personnel que cette plainte est susceptible de soulever. Afin de mieux comprendre le fonctionnement du « pop-up » objet du litige, et le rôle d'Apple au sein de l'écosystème, l'ADLC a adressé une demande d'informations complémentaires à la société Apple, qui a transmis ses réponses dans un courrier en date du 9 décembre 2020 (annexe 2).

A titre liminaire, la Commission attire l'attention de l'ADLC sur le fait que le dispositif, objet de la plainte concerne les traitements de données mis en œuvre par les éditeurs d'applications et leurs partenaires à des fins de traçage publicitaire, tel que défini par la société Apple, que ceux-ci se fassent *via* l'utilisation de l'identifiant publicitaire du terminal (IDFA) ou au moyen de technologies alternatives. Il couvre ainsi le fait de lier les données collectées sur un utilisateur ou son terminal avec les données collectées sur les applications, sites web ou hors ligne par des tiers (éditeurs d'applications, etc.) ainsi que le partage avec des courtiers en données à ces fins.

I. Le fonctionnement des identifiants publicitaires mobiles : l'exemple de l'IDFA

L'« Identifier For Advertisers » (IDFA) est un identifiant attribué de manière logicielle à chaque appareil par le système d'exploitation iOS de la société Apple. Il s'agit, en pratique, d'une série de caractères hexadécimaux¹ créée dans le but de permettre aux acteurs publicitaires d'identifier l'appareil de manière unique dans chaque application installée dessus.

L'IDFA a été introduit, en 2012, dans la version 6 d'iOS, afin de remplacer l'usage d'identifiants matériels tel que l'IMEI², l'UDID³ ou l'adresse MAC⁴ massivement utilisés par les acteurs publicitaires. Contrairement aux identifiants matériels, l'IDFA est révoquant, et iOS offre la possibilité aux utilisateurs de limiter son usage en utilisant l'option « suivi publicitaire limité » depuis le panneau de configuration iOS. Jusqu'en 2016 (avec iOS 10), ce « suivi publicitaire limité » informait les tiers publicitaires du

¹ Identifiant de type « Universally Unique Identifier » (UUID) de 32 caractères hexadécimaux, par exemple « 123e-4567-e89b-12d3-a456-4266-1417-4000 ».

² L'« *International Mobile Equipment Identity* » est un numéro qui permet d'identifier de manière unique chacun des terminaux de téléphonie mobile et permet à l'opérateur d'un réseau mobile d'identifier le terminal appelant et ainsi de l'autoriser, ou non, à se connecter au réseau.

³ Il s'agit d'un identifiant unique de 40 caractères, propre à Apple, permettant d'identifier un terminal iOS. Cet identifiant sert notamment aux développeurs d'applications afin de donner accès à leur application avant de la soumettre dans l'App Store.

⁴ Une adresse MAC (pour « Media Access Control »), parfois appelée « adresse physique », est un identifiant physique stocké dans une carte réseau ou une interface réseau similaire.

choix de l'utilisateur sans toutefois en limiter techniquement l'accès. Depuis iOS 10, ce « suivi publicitaire limité » empêche tout suivi de l'utilisateur, en fixant sa valeur à zéro.

1. Différences entre l'IDFA et les cookies web

A l'inverse des *cookies*, dont la valeur est fixée indépendamment pour chaque tiers publicitaire, l'IDFA est généré aléatoirement lors du premier démarrage du téléphone et est le même pour tous les tiers. L'IDFA facilite ainsi la mise en relation entre ces tiers, des données collectées relatives à un individu. Couplé à un environnement authentifié, il permet également de relier ces données à une activité sur d'autres terminaux informatiques de l'utilisateur depuis lesquels celui-ci s'est également authentifié. Ceci peut permettre à des acteurs publicitaires de valoriser les données collectées sur un utilisateur dans le contexte d'une application en lui proposant des publicités ciblées dans d'autres applications. Cela augmente également l'intrusion potentielle de cette technologie dans la vie privée des utilisateurs d'iPhones.

Si les *cookies* peuvent être utilisés pour des finalités non publicitaires (dont certaines peuvent être indispensables au bon fonctionnement du site⁵), l'IDFA est uniquement associée à des finalités publicitaires. La désactivation de l'IDFA n'affecte donc pas le bon fonctionnement des sites et applications.

2. L'utilisation de l'IDFA est limitée aux finalités publicitaires

La société Apple indique ainsi dans sa documentation que les usages autorisés de cet identifiant sont les suivants :

- **la maîtrise de la répétition publicitaire (aussi appelé le « capping ») :** elle permet de limiter la fréquence et le nombre total d'affichage d'une publicité pour un utilisateur, à travers toutes les applications utilisées ;
- **l'attribution :** elle permet d'attribuer un acte d'achat ou d'installation d'un logiciel, effectué dans le contexte d'une application, au visionnage d'une publicité dans une autre application par l'utilisateur ;
- **l'estimation du nombre d'utilisateurs uniques ayant vu une publicité,** en ne comptant qu'une seule fois un utilisateur ayant vu une publicité dans plusieurs applications ;
- **le profilage :** il permet de combiner, dans un profil publicitaire unique, les données collectées sur les usages et les intérêts d'un utilisateur à travers toutes les applications qu'il utilise, voire de les lier avec des données obtenues lors de son usage d'une plateforme authentifiée (par exemple, un réseau social, un site de e-commerce, etc.) ;
- **le reciblage :** il permet d'afficher, dans une application, une publicité liée à un acte d'achat interrompu dans le contexte d'une autre application, afin de pousser l'utilisateur à finaliser son achat.

⁵ Par exemple, pour réaliser l'authentification ou la conservation des articles dans un panier d'achat.

II. La réglementation en matière de traitements publicitaires : l'articulation entre la directive « ePrivacy » et le règlement général sur la protection des données

Les traitements de données mis en œuvre à des fins publicitaires sont soumis à deux réglementations posant des conditions exigeantes en matière de contrôle des utilisateurs sur leurs données :

- le règlement général sur la protection des données (RGPD), qui s'applique dès lors que les données collectées et traitées peuvent être qualifiées de données à caractère personnel ;
- les dispositions nationales transposant la directive 2002/58/CE sur la protection de la vie privée dans le secteur des communications électroniques (ci-après, la directive « ePrivacy »), qui s'appliquent en complément des règles générales du RGPD dès lors que certaines opérations sont mises en œuvre *via* un service de communications électroniques accessible au public.

1. Le traitement de données à caractère personnel entraîne l'application du RGPD

❖ La collecte de données à caractère personnel

L'objectif de la publicité personnalisée est de « cibler » un individu, en adaptant à ses centres d'intérêts supposés le contenu qui lui est affiché. Afin de lier un utilisateur à un profil, deux techniques sont possibles :

- **le profil de l'utilisateur ne contient pas de données directement identifiantes** (nom, prénoms, adresse électronique, etc.) : les informations collectées sont rattachées à l'utilisateur par le biais d'un identifiant unique qui permet de le suivre dans le temps, enrichissant ainsi progressivement son profil avec de nouvelles informations collectées au fil de sa navigation ;
- **le profil de l'utilisateur est directement relié à des données directement identifiantes** : cette association avec des données identifiantes est généralement réalisée par le biais de services sur lesquels l'utilisateur est authentifié (univers dits « *logués* »), ou à l'occasion de transactions qu'il peut effectuer sur des sites web (souscription à une lettre d'information, achat sur un site de vente en ligne) qui permettent aux opérateurs d'associer l'identifiant publicitaire de ce dernier à des données de contact (nom, prénom, adresse électronique, etc.) ainsi que des données socio-démographiques. Cette technique permet notamment de cibler l'utilisateur sur ses différents appareils (ordiphone, ordinateur, tablette) depuis lesquels il s'est également authentifié.

Selon les termes de la loi, les données peuvent être qualifiées de données à caractère personnel dès lors qu'elles se rapportent à une personne physique identifiée ou identifiable, directement ou indirectement, notamment par référence à un identifiant (un identifiant publicitaire, par exemple) ou à plusieurs éléments qui lui sont spécifiques.

❖ **Le caractère intrusif des traitements publicitaire exige une attention particulière quant au respect des obligations du RGPD**

Les technologies numériques modernes, et notamment celles relatives à l'analyse de grandes masses de données, permettent aux réseaux publicitaires de tracer les personnes et de combiner les informations provenant de sources diverses concernant leur comportement, afin de constituer des profils détaillés sur leurs centres d'intérêt. Ces profils peuvent alors servir à leur adresser des publicités personnalisées, à un endroit et à un moment pertinents pour l'annonceur.

Le RGPD doit permettre aux utilisateurs de conserver le contrôle sur leurs données à caractère personnel collectées en ligne, d'une part, en imposant des obligations aux acteurs qui ont une influence sur leur traitement et, d'autre part, en octroyant des droits aux utilisateurs pour leur en assurer la maîtrise.

La Commission attire l'attention de l'ADLC sur le fait que le respect de ces réglementations doit être adapté aux risques présentés par le traitement de données sur les droits et libertés fondamentaux des personnes. Dès lors, le caractère particulièrement intrusif de la publicité en ligne (extrême personnalisation de certains modèles de publicité, traitement des données par un nombre considérable d'acteurs de l'écosystème publicitaire, combinaison de plusieurs sources de données, etc.) doit justifier une attention particulière quant au respect de certaines obligations : le respect des obligations en matière de transparence devra être renforcé, une analyse d'impact sur la protection des données devra être réalisée lorsque le traitement est susceptible de présenter un risque élevé, etc.

2. L'utilisation de technologies encadrées par les dispositions nationales transposant la directive « ePrivacy »

La publicité en ligne repose sur l'accès à l'équipement terminal de l'utilisateur⁶ (ordiphone, ordinateur fixe ou mobile, télévision connectée, etc.), qu'il s'agisse d'accéder, par voie de transmission électronique, à des informations déjà stockées dans cet équipement (par exemple, un identifiant publicitaire) ou à y inscrire des informations.

Le législateur a particulièrement encadré ces actions compte tenu, d'une part, du fait que ce terminal personnel est attaché à la sphère intime de l'individu et, d'autre part, que ces opérations interfèrent avec les actions réalisées par l'utilisateur depuis un nombre croissant d'objets du quotidien. Ainsi, il résulte de l'article 82 de la loi du 6 janvier 1978 modifiée (ci-après la loi « Informatique et Libertés »), qui transpose en droit national l'article 5.3 de la directive « ePrivacy », que toute opération de lecture ou d'écriture nécessaire à la constitution d'un profil d'utilisateur et à la fourniture de publicité ciblée, requiert un accord préalable de l'utilisateur, qu'il y ait ou non traitement de données à caractère personnel.

⁶ L'article 1^{er} de la directive 2008/63/CE du 20 juin 2008 susvisée définit l'équipement terminal comme « *tout équipement qui est connecté directement ou indirectement à l'interface d'un réseau public de télécommunications pour transmettre, traiter ou recevoir des informations ; dans les deux cas, direct ou indirect, la connexion peut être établie par fil, fibre optique ou voie électromagnétique ; une connexion est indirecte si un appareil est interposé entre l'équipement terminal et l'interface du réseau public* ».

3. Les exigences des textes en matière de consentement de l'utilisateur

La Commission rappelle que le consentement prévu par les dispositions de l'article 82 de la loi « Informatique et Libertés », lues à la lumière de l'article 5 de la directive « ePrivacy » et de l'article 94 du RGPD, renvoie à la définition et aux conditions prévues aux articles 4(11) et 7 du RGPD.

L'utilisateur devra ainsi avoir l'opportunité, avant toute opération, de manifester sa volonté, de manière libre, spécifique, éclairée et univoque, par une déclaration ou par un acte positif clair.

La Commission a publié, le 1^{er} octobre 2020, des lignes directrices et une recommandation afin d'aider les acteurs à se conformer aux règles protégeant les données à caractère personnel et la vie privée des internautes, selon un standard robuste et durable. Si les lignes directrices se limitent à synthétiser et expliciter le droit applicable à l'utilisation de cookies et autres traceurs, la recommandation propose des exemples concrets de modalités permettant notamment de recueillir un consentement conforme aux règles applicables (annexes 3 et 4).

III. Le « pop-up » de la société Apple permettrait aux éditeurs d'applications de recueillir un consentement valide, au sens de la réglementation européenne, pour les traitements à finalités publicitaires

Si la société Apple a précisé que le « pop-up » objet du litige n'a pas été conçu afin de permettre aux développeurs de se conformer à leurs obligations légales, elle affirme cependant que le choix offert au consommateur de donner explicitement son autorisation à tout traçage publicitaire peut aider les éditeurs d'applications à se conformer à la réglementation.

La Commission s'est alors interrogée sur le fait de savoir dans quelle mesure le dispositif permettrait, en pratique, aux éditeurs d'applications de recueillir le consentement imposé par les dispositions de l'article 82 de la loi « Informatique et Libertés ».

1. Le « pop-up » proposé par la société Apple se distingue positivement de certaines interfaces non conformes à la réglementation

La Commission relève que, à certains égards, le « pop-up » proposé par la société Apple se distingue des interfaces actuellement observées sur un nombre considérable de sites web et d'applications mobiles non conformes à la réglementation.

Tout d'abord, le « pop-up » proposé par la société Apple permet d'accepter ou de refuser le traçage avec le même degré de simplicité *via* l'inclusion de boutons « permettre le suivi » et « demander à l'application de ne pas permettre le suivi » (traduction libre) au même niveau et sur le même format. Ces modalités constituent un moyen simple et clair pour permettre à l'utilisateur d'exprimer son refus aussi facilement que son consentement, comme l'a souligné l'a Commission dans sa recommandation relative aux *cookies* et autres traceurs.

La capacité de refuser aussi facilement le suivi que d'y consentir est un élément structurant du contrôle offert à l'utilisateur sur son terminal ainsi que, par voie de conséquence, sur ses données à caractère personnel. Or, la Commission observe que de nombreuses interfaces de recueil des choix ne permettent pas, encore aujourd'hui, de respecter la réglementation sur ce point dès lors que plusieurs actions sont, en général, nécessaires pour « paramétrer » un refus de consentir alors qu'un seul clic permet de consentir au traçage.

Par ailleurs, la Commission estime que la mention du suivi au sein des différentes applications et sites web utilisés par ce dernier et détenus par d'autres éditeurs est une information essentielle pour permettre à l'utilisateur de prendre conscience de l'ampleur potentielle de la collecte de données qui ira alimenter son profil à des fins publicitaires et donc d'être éclairé sur la portée de son choix.

Enfin, elle considère favorablement le fait que ce « pop-up » permette un recueil du consentement sur chacune des applications concernées par ce suivi, ce qui contribue également à garantir que l'utilisateur soit pleinement conscient de la portée de son consentement.

2. L'éditeur de l'application peut compléter le « pop-up » pour recueillir un consentement valide au sens de la réglementation applicable

Les associations requérantes mettent en avant, dans leur saisine, que le « pop-up », objet du litige, ne permet pas de collecter un consentement valide au sens du RGPD et que, par conséquent, les éditeurs d'applications se verront contraint d'utiliser d'autres solutions en complément du dispositif imposé par la société Apple. Plus précisément, selon les associations requérantes, le « pop-up » d'Apple ne permet pas d'obtenir le consentement éclairé et spécifique des utilisateurs et de retirer l'autorisation de suivi aussi facilement que celle-ci puisse être accordé.

❖ S'agissant du caractère éclairé du consentement de l'utilisateur

Conformément à l'article 4(11) du RGPD, l'utilisateur doit être mis en mesure de comprendre l'usage qui sera fait de ses données à caractère personnel avant de donner son consentement. S'il n'est pas contesté que les éditeurs d'applications peuvent afficher leurs propres messages avant l'apparition du « pop-up » proposé par la société Apple⁷, la Commission s'est interrogée sur la possibilité pour ces derniers de venir ajouter, aux informations présentées par défaut à l'utilisateur, les éléments d'informations indispensables au recueil d'un consentement éclairé.

La Commission prend acte des précisions apportées par la société Apple selon lesquelles les éditeurs d'application seront, en effet, en mesure de compléter le « pop-up » afin, notamment, d'informer les utilisateurs sur l'utilisation qui sera faite des données collectées *via* les traceurs⁸ et tenter de les inviter à consentir.

⁷ Les éditeurs d'application conservent la maîtrise de l'affichage du « pop-up » qui choisit de demander ou non l'autorisation de l'internaute pour le tracer et décide donc si (et quand) la sollicitation s'affiche à l'écran.

⁸ La société Apple précise que les « développeurs peuvent modifier le texte qui s'affiche en non-gras dans le pop-up, et qu'ils ont toute liberté pour modifier cette partie de la fenêtre ».

A la lumière de ces éléments, il apparaît, en l'état des informations dont dispose la Commission, que le dispositif proposé par la société Apple permettrait aux éditeurs d'application, sous réserve d'intégrer les éléments d'informations légalement exigibles, que la CNIL a rappelés à l'article 2 de ses lignes directrices « *cookies* et autres traceurs », de collecter un consentement éclairé tel qu'exigé par la réglementation applicable. Elle rappelle néanmoins qu'afin de répondre aux exigences de transparence requises par la réglementation, l'information présentée à l'utilisateur devra être adaptée aux contraintes de l'environnement mobile (notamment la taille de l'écran). Par exemple, une approche à plusieurs niveaux, telle que recommandée par le Comité européen de la protection des données dans ses lignes directrices sur la transparence⁹, peut contribuer à améliorer la clarté de l'information ainsi délivrée.

❖ S'agissant du respect des exigences relatives au retrait du consentement

La Commission rappelle que le RGPD impose au responsable du traitement (l'éditeur de l'application notamment) de permettre à l'utilisateur de retirer son consentement, à tout moment, aussi facilement que de le donner.

La Commission prend acte des précisions apportées par la société Apple selon lesquelles l'utilisateur sera en capacité de revenir sur ses choix, application par application, au sein des réglages offerts par le système d'exploitation (rubrique « confidentialité », section « suivi »)¹⁰. Elle attire l'attention de l'ADLC sur le fait que si l'éditeur de l'application se repose sur les réglages offerts par la société Apple, il devrait néanmoins intégrer un mécanisme permettant à l'utilisateur d'y accéder directement dans l'application concernée, afin de s'assurer que le retrait ne nécessite pas plus d'efforts que lorsque l'utilisateur a donné son consentement *via* un simple « clic » sur le « pop-up ». A défaut, il est nécessaire de mettre en œuvre une solution répondant aux exigences légales de retrait aisé du consentement.

IV. Les évolutions annoncées par la société Apple sont-elles le résultat d'une obligation posée par la réglementation ?

La Commission s'est interrogée sur le fait de savoir s'il relève de la responsabilité de la société Apple, au sens du RGPD, de s'assurer qu'un consentement valide soit collecté avant que les éditeurs d'application puissent tracer l'utilisateur à des fins publicitaires (notamment en utilisant l'IDFA qui permet un tel suivi).

La qualification de la société quant aux traitements publicitaires mis en œuvre par les éditeurs d'application et les acteurs publicitaires s'avère déterminante pour tirer les conséquences quant aux obligations susceptibles de peser sur elle. En effet, la notion de responsable du traitement joue un rôle crucial dans l'application du RGPD et de l'article 82 de la loi « Informatique et libertés » puisqu'elle détermine la répartition des obligations entre chaque acteur intervenant dans le traitement de données mis en œuvre et, notamment, s'agissant du recueil du consentement de l'utilisateur lorsque celui-ci en est une condition de licéité. Deux hypothèses doivent ainsi être distinguées.

⁹ Lignes directrices sur la transparence au sens du règlement (UE) 2016/679. Groupe de travail « Article 29 », WP260 rev.01, endossées par le Comité européen de la protection des données (CEPD). Disponible ici : https://www.cnil.fr/sites/default/files/atoms/files/wp260_guidelines-transparence-fr.pdf

¹⁰ Ces modalités sont identiques à celles déjà disponibles pour d'autres catégories de données gérées par le système d'exploitation iOS comme, par exemple, les contacts de l'utilisateur ou encore son calendrier et sa localisation.

1. Hypothèse 1 : la société Apple est responsable conjoint des opérations de traitement mises en œuvre à des fins de traçage publicitaire par les éditeurs d'applications

Il est évident que les sociétés exploitant les applications proposées sur les équipements de marque Apple et recourant à du ciblage publicitaire sont responsables de ces traitements. Cependant, il est possible qu'il y ait plusieurs responsables conjoints du traitement lorsque plusieurs acteurs sont impliqués dans les opérations de traitement concernées et que ces derniers participent conjointement à la détermination des finalités et des moyens de telles opérations.

Si une analyse, au regard des circonstances de l'espèce, venait à conclure à une responsabilité conjointe, alors l'obligation de collecter un consentement valide, en application de l'article 82 de la loi « Informatique et Libertés », serait susceptible de reposer tant sur l'éditeur de l'application que sur la société Apple.

Conformément à l'article 26 du RGPD, qui régit les relations entre responsables conjoints du traitement, il appartient aux différentes parties (dans cette hypothèse, la société Apple et l'éditeur de l'application) de définir entre elles, de manière transparente, leurs obligations respectives. L'objectif est d'assurer, lorsque plusieurs acteurs sont impliqués, notamment dans des environnements de traitement de données complexes, que la responsabilité du respect des règles en matière de protection des données soit clairement répartie. Les responsables conjoints d'un traitement de données disposent d'un certain degré de flexibilité dans la répartition des obligations entre eux, à condition qu'ils garantissent le plein respect du RGPD en ce qui concerne le traitement¹¹.

Dès lors, dans une telle hypothèse, l'initiative d'Apple pourrait être analysée comme une réponse à l'obligation d'assurer le recueil du consentement de l'utilisateur à des fins de traçage publicitaire, que celui-ci passe par l'usage de l'IDFA ou *via* des méthodes alternatives impliquant également un accès au terminal de l'utilisateur.

Afin d'apprécier la qualification d'Apple en tant que responsable conjoint du traitement de données publicitaires mis en œuvre par les éditeurs d'application, il convient tout d'abord de savoir si la société Apple exploite ces mêmes données dans le cadre de ces mêmes opérations de traitement. Si la réponse à cette question est affirmative, il conviendra ensuite de s'interroger sur la présence d'une participation conjointe à la détermination des finalités et des moyens du traitement, que cela prenne la forme d'une décision commune¹² ou bien résulte de décisions convergentes¹³ de la société Apple et des éditeurs d'applications.

¹¹Les autorités de protection des données, telles que la CNIL, ne sont pas liées par les termes de l'accord et pourront faire une analyse *in concreto* des obligations de chacun, c'est-à-dire au regard des circonstances de l'espèce.

¹² La participation conjointe par le biais d'une décision commune signifie décider ensemble et implique une intention commune.

¹³Les décisions peuvent être considérées comme convergentes sur les finalités et les moyens si elles sont complémentaires et nécessaires pour que le traitement soit mis en œuvre d'une manière telle qu'elles ont un impact réel/tangible sur la détermination des finalités et des moyens du traitement. Un critère important pour identifier des décisions convergentes est de savoir si le traitement ne serait pas possible sans la participation des deux parties, en ce sens que le traitement effectué par chacune d'elles est inextricablement lié.

En l'état du dossier, la Commission relève qu'Apple déclare ne traiter en aucune façon l'IDFA ou aucun autre identifiant publicitaire, ni aucune donnée issue des différentes techniques de suivi des comportements des utilisateurs, ni directement pour elle-même, ni par l'intermédiaire des applications utilisant sa technologie. Cependant, la Commission ne souhaite pas, à ce stade, se positionner sur la qualification d'un acteur aussi structurant qu'Apple quant aux traitements publicitaires mis en œuvre par les éditeurs d'applications. D'une part, elle ne dispose pas des informations nécessaires à une telle analyse, qui nécessiterait des investigations complémentaires (contrôles officiels, notamment). De surcroît, la Commission attire l'attention de l'ADLC sur le fait que plusieurs associations de défense des libertés numériques ont déposé des réclamations à l'encontre de la société Apple auprès de plusieurs autorités de protection des données européennes, s'agissant de l'usage de l'IDFA. La qualification de la société Apple doit notamment faire l'objet d'une décision de « *l'autorité chef de file*¹⁴ » prise dans le cadre du mécanisme de coopération prévu par le RGPD, ce qui permettra aux autorités de protection des données, dont la CNIL, d'avoir une position harmonisée sur le sujet.

2. Hypothèse 2 : la société Apple n'est pas responsable conjoint des opérations de traitements publicitaires mis en œuvre par l'ensemble des éditeurs d'application qui opèrent un suivi des utilisateurs

En l'absence d'une telle qualification, la responsabilité d'Apple quant à la collecte d'un consentement valide pour les opérations de traitement concernées ne pourra être que limitée, voire inexistante, sur le fondement de la réglementation relative à la protection des données.

Toutefois, le RGPD et les dispositions nationales transposant la directive « ePrivacy » n'interdisent en aucun cas aux concepteurs de logiciels de fournir voire d'imposer son design sur la fenêtre de recueil des choix. La réglementation encourage d'ailleurs fortement ces derniers à prendre en compte le droit à la protection des données lors de l'élaboration et de la conception de leurs produits et à s'assurer que les responsables du traitement et les sous-traitants sont en mesure de s'acquitter des obligations qui leur incombent en matière de protection des données¹⁵.

Par ailleurs, la Commission considère que les évolutions proposées par la société Apple peuvent avoir un véritable bénéfice, tant pour les utilisateurs que pour les éditeurs d'application.

En premier lieu, le dispositif offrirait aux utilisateurs un meilleur contrôle sur leurs données à caractère personnel en leur permettant, d'une part, d'exprimer leurs choix de manière simple et éclairé (sous réserve des éléments rappelés ci-dessus) et, d'autre

¹⁴ Le RGPD prévoit que les organismes qui mettent en œuvre des traitements « transfrontaliers » peuvent bénéficier du mécanisme du « guichet unique » et disposer ainsi d'un seul interlocuteur pour toutes leurs activités de traitement sur le territoire européen : l'autorité « chef de file ». L'établissement principal d'Apple se situant en Irlande, l'autorité irlandaise de protection des données est réputée être l'autorité chef de file de la société.

¹⁵ Le considérant 78 du RGPD incite les fabricants de produits, les prestataires de services et les producteurs d'applications à implémenter les principes de protection des données dès la conception et de protection des données par défaut.

part, en empêchant techniquement¹⁶ et/ou contractuellement¹⁷ aux éditeurs d'application de tracer l'utilisateur sans son autorisation. Par ailleurs, la standardisation de la fenêtre de recueil des choix et son utilisation par l'ensemble des éditeurs d'applications qui mettent en œuvre un traçage à des fins publicitaires permet de faciliter, de manière significative, l'exercice des choix de l'utilisateur.

En second lieu, la Commission relève que le « pop-up » incriminé peut aider de nombreux petits éditeurs à se conformer à l'obligation posée par les dispositions de l'article 82 de la loi « Informatique et Libertés » en leur fournissant un outil simple leur permettant de recueillir un consentement valide pour leurs opérations de traçage publicitaire.

En tout état de cause, la Commission n'est pas compétente pour se prononcer sur le respect des dispositions relevant du droit des contrats ou du droit de la concurrence, notamment dans les situations où il est susceptible d'exister un déséquilibre entre un éditeur d'applications et une plateforme en position dominante sur le marché concerné. Il appartiendra ainsi aux autorités compétentes en la matière de se prononcer sur le caractère abusif ou non de la solution proposée par la société Apple aux éditeurs d'applications mobiles.

Pour conclure, le dispositif objet du litige ne sera considéré comme le résultat d'une obligation susceptible de peser sur la société Apple (en fonction de la répartition des responsabilités) que si elle devait être qualifiée de responsable conjoint du traitement mis en œuvre par les éditeurs d'application. Néanmoins, à défaut, la Commission relève que la réglementation relative à la protection des données n'empêche pas la société Apple de mettre en œuvre un dispositif permettant d'interdire aux éditeurs d'application de tracer l'utilisateur sans consentement, d'autant plus lorsque celui-ci est imposé par la réglementation.

V. Les traitements mis en œuvre par Apple, pour son propre compte, au sein de sa plateforme publicitaire nécessitent-ils un consentement ?

Lancée en 2016, la plateforme publicitaire d'Apple permet aux éditeurs qui souhaitent augmenter les téléchargements de leurs applications, et ainsi acquérir de nouveaux utilisateurs, de cibler ces derniers avec des publicités d'installation d'applications affichées notamment en haut des résultats de recherche sur l'Apple Store¹⁸.

Les associations requérantes indiquent, dans leur saisine, qu'Apple ne s'applique pas les mêmes exigences qu'il entend imposer aux éditeurs et exploitants d'application, puisque les traitements publicitaires mis en œuvre par la société dans le cadre de sa plateforme ne reposeraient pas, selon elles, sur un consentement exprès de l'utilisateur. La Commission s'est donc interrogée sur l'application des dispositions de l'article 82 de la loi « Informatique et Libertés » aux traitements publicitaires mis en œuvre par la société Apple, ainsi que sur l'existence d'un accord préalable de l'utilisateur aux éventuelles opérations de lecture ou d'écriture.

¹⁶ Apple ne permettra pas, à l'éditeur de l'application, d'accéder à l'IDFA sans que l'utilisateur ait consenti au sein du « pop-up » que l'éditeur aura dû afficher pour recueillir l'autorisation de l'utilisateur.

¹⁷ L'utilisation de méthodes alternatives de traçage publicitaire sans consentement de l'internaute pourront conduire à exclure l'application de l'Apple Store.

¹⁸ Il s'agit de liens sponsorisés qui apparaissent lorsque l'utilisateur effectue une recherche pour une application.

1. Tous les acteurs sont soumis aux mêmes règles s'agissant de la protection des données à caractère personnel

La Commission attire l'attention de l'ADLC sur le fait que la réglementation « ePrivacy » s'applique de la même façon aux grandes plateformes numériques qui collectent massivement des données à l'intérieur d'univers « logués » qu'aux éditeurs d'applications qui collectent les données dans des environnements où les utilisateurs ne sont pas authentifiés. Ainsi, s'il existe des différences objectives – tenant aux choix de modèles économiques, au caractère intrusif des traitements potentielles mis en œuvre, ou à l'attraction qu'ils peuvent exercer sur les consommateurs – les règles juridiques sont les mêmes pour tous.

2. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

3. [REDACTED]

[REDACTED]

²⁰ En effet, comme rappelé précédemment, le « pop-up » ne concerne que les traitements impliquant un traçage publicitaire de l'utilisateur tel que défini par la société Apple.

[REDACTED]



La Présidente

Marie-Laure DENIS