RÉPUBLIQUE FRANÇAISE

Autorité de la concurrence

Avis n° 23-A-20 du 4 décembre 2023 relatif au projet de recommandation de la CNIL relative aux applications mobiles

L'Autorité de la concurrence (commission permanente),

Vu la lettre enregistrée le 22 mars 2023 sous le numéro 23/0022 A, par laquelle la Commission Nationale de l'Informatique et des Libertés (CNIL) a saisi l'Autorité de la concurrence d'une demande d'avis concernant son projet de recommandation relative aux applications mobiles ;

Vu le Traité sur le fonctionnement de l'Union européenne ;

Vu le livre IV du code de commerce ;

Vu les autres pièces du dossier ;

Les représentants de deux sociétés entendues en leur qualité d'éditeurs d'applications mobiles sur le fondement des dispositions du deuxième alinéa de l'article L. 463-7 du code de commerce ;

Les rapporteures, la rapporteure générale adjointe, les représentants de la CNIL et le commissaire du Gouvernement entendus lors de la séance de l'Autorité de la concurrence du 18 octobre 2023 ;

Est d'avis de répondre à la demande présentée dans le sens des observations suivantes :

Résumé[1]

Sur le fondement de l'article 15 de la loi n° 2017-55 du 20 janvier 2017 portant statut général des autorités administratives indépendantes et des autorités publiques indépendantes, l'Autorité de la concurrence (ci-après, « l'Autorité ») a été saisie par la Commission Nationale de l'Informatique et des Libertés (ci-après, « CNIL ») pour avis portant sur un projet de recommandation relative aux applications mobiles (ci-après, le « projet »).

Les applications mobiles, logiciels applicatifs distribués dans l'environnement des téléphones mobiles multifonctions et tablettes, constituent l'un des principaux moyens d'accès à des contenus et des services numériques à partir de ces terminaux mobiles. Elles permettent d'y ajouter des fonctionnalités ou services supplémentaires dans des domaines très divers (services de réseaux sociaux, de divertissement, d'achats à distance, mobilité, services bancaires, etc.).

L'utilisation d'applications mobiles permet le traitement de grandes quantités de données personnelles. Selon la CNIL, si les principes et obligations en matière de protection des données et de la vie privée (ci-après, « protection de la vie privée ») sont désormais bien connus des opérateurs de sites internet et font déjà l'objet de recommandations, leur mise en œuvre dans le contexte des applications mobiles serait parfois incertaine.

Dans ce contexte, le projet de la CNIL vise à apporter davantage de sécurité juridique aux acteurs et à favoriser des bonnes pratiques au bénéfice des utilisateurs. Ce projet clarifie en particulier les qualifications et responsabilités des différents acteurs de l'écosystème des applications mobiles au regard de la réglementation applicable en matière de protection de la vie privée. Il rappelle en premier lieu, les principales obligations de ces acteurs au regard du Règlement général de la protection des données (ci-après, « RGPD ») et de la loi dite Informatique et Libertés[2] et édicte, en second lieu, une série de conseils et de bonnes pratiques dont la CNIL préconise la mise en œuvre.

La structure concurrentielle du secteur des applications mobiles se caractérise par la présence d'acteurs verticalement intégrés tout au long de la chaîne de valeur des applications mobiles et qui ont mis en place des écosystèmes distincts. En effet, Alphabet Inc. et Apple sont à la fois fournisseurs de systèmes d'exploitation (ci-après, « OS »), de magasins d'applications et de kits de développements logiciels, éditeurs, développeurs et fournisseurs d'autres services. En tant que fournisseur d'OS et/ou de magasins d'applications, ces acteurs établissent au sein de leur écosystème, des règles d'accès spécifiques. En outre, ces acteurs ont récemment été désignés « *contrôleurs d'accès* » au sens du règlement sur les marchés numériques (« *Digital Markets Act* », ci-après, le « DMA ») par la Commission européenne pour plusieurs services de plateforme essentiels, dont leurs OS pour terminaux mobiles (Google Android pour Alphabet et iOS pour Apple) et leurs services d'intermédiation de magasins d'applications (Google Play Store pour Alphabet et App Store pour Apple). Ce règlement, en vigueur depuis novembre 2022 et appliqué depuis mai 2023, régit certains services des contrôleurs d'accès, à savoir de grandes plateformes en ligne qui constituent un point d'accès majeur entre les entreprises utilisatrices et les consommateurs, afin de garantir la contestabilité et l'équité des marchés dans le secteur numérique. De plus, ces acteurs

[1] Ce résumé a un caractère strictement informatif. Seuls font foi les motifs de l'avis numérotés ci-après.

[2] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n° 2018-493 du 20 juin 2018.

verticalement intégrés sont susceptibles de détenir une position dominante sur certains marchés de la chaîne de valeur des applications mobiles.

L'Autorité et la CNIL partagent une ambition commune de protection des données personnelles et de la vie privée et du respect de la concurrence. En particulier, ces deux politiques présentent une certaine convergence d'objectifs, en ce qu'elles sont, *in fine*, mises en œuvre au bénéfice des usagers.

En ce sens, l'Autorité considère que le projet de la CNIL doit être salué en ce qu'il vise à répondre à un besoin de clarification exprimé par les acteurs du secteur et, *in fine*, à favoriser une meilleure protection des données personnelles de l'utilisateur.

En particulier, l'Autorité considère qu'une meilleure information des acteurs de la chaîne de valeur des applications mobiles concernant la mise en œuvre de la réglementation sur la protection de la vie privée est source de transparence des marchés et de réduction des barrières à l'entrée. L'Autorité salue également les recommandations de la CNIL visant à favoriser des règles d'accès transparentes, en particulier les recommandations relatives à la transparence des processus de revue des magasins d'applications.

S'agissant des utilisateurs, l'Autorité souligne que plusieurs recommandations encouragent une meilleure transparence de l'information des utilisateurs sur la collecte et l'utilisation de leurs données personnelles. Sur ce point, l'Autorité considère qu'une meilleure transparence de l'information est de nature à éclairer les consommateurs lors de leurs décisions et à favoriser l'exercice plus libre de la concurrence sur le paramètre de la protection de la vie privée.

Toutefois, il peut parfois exister des tensions entre les objectifs des politiques de protection de la vie privée et de concurrence. Ainsi, les dispositions du RGPD, qui visent en premier chef la protection de la vie privée, sont le fruit d'une mise en balance entre plusieurs intérêts légitimes, y compris la nécessité de ne pas affecter excessivement l'efficacité des marchés. L'Autorité estime que des mesures de protection de la vie privée qui iraient au-delà de ce qui est strictement imposé par le RGPD ne sont pas illicites en soi. Toutefois, afin d'éviter qu'elles ne nuisent à la bonne efficacité économique des marchés, il est essentiel qu'elles soient définies et mises en œuvre en évitant d'engendrer des effets anticoncurrentiels qui ne seraient pas contrebalancés par un gain suffisant pour les consommateurs. Ceci est particulièrement important lorsque de telles mesures sont mises en œuvre par des opérateurs dominants, lesquels doivent veiller à ne pas porter atteinte, par leur comportement, à une concurrence effective et non faussée et, partant, doivent s'assurer que leurs règles d'accès ou de fonctionnement soient proportionnées et appliquées de manière objective, transparente et non discriminatoire.

Or, l'Autorité observe que le projet accorde aux fournisseurs d'OS et aux magasins d'applications un rôle important en matière de protection de la vie privée qui ne découle pas directement d'obligations conférées par la réglementation en vigueur relative à la protection de la vie privée, et notamment par le RGPD.

Partant de ces constatations, l'Autorité considère que le projet devrait, dans son approche, davantage tenir compte de la structure concurrentielle du secteur, et en particulier de la position de certains acteurs. Dans ce contexte, l'Autorité appelle l'intérêt de la CNIL à ce que ses recommandations ne confèrent pas un pouvoir supplémentaire à des acteurs disposant déjà d'un fort pouvoir de marché, notamment à ceux qui ont été désignés contrôleurs d'accès pour certains services ou qui pourraient être considérés comme étant en position dominante, ces acteurs pouvant être susceptibles de s'appuyer sur ces recommandations à des fins anticoncurrentielles. De plus, l'Autorité invite la CNIL à prêter

une attention particulière à ce que ses recommandations n'aient pas l'effet de déléguer sa compétence, en tant que régulateur national, aux contrôleurs d'accès, au risque de renforcer les asymétries de pouvoir de marché au bénéfice de ces derniers.

L'Autorité considère également souhaitable que la CNIL mentionne expressément que ses recommandations s'appliquent de la même manière aux applications mobiles propriétaires des fournisseurs d'OS ou de magasins d'applications qu'aux applications tierces, afin d'éviter que celles-ci soient utilisées par certains opérateurs pour mettre en œuvre un traitement différencié susceptible d'avantager les applications mobiles propriétaires.

En outre, dans la mesure où les bonnes pratiques préconisées par la CNIL ne résulteraient pas d'une approche harmonisée entre les différentes autorités nationales de régulation de la protection de la vie privée, l'Autorité accorde une importance particulière au fait que ces recommandations ne viennent pas créer des barrières à l'entrée supplémentaires pour de nouveaux entrants sur le marché français ni de désavantage en termes de coûts ou de contraintes pour les entreprises établies en France.

Enfin, l'Autorité invite la CNIL à s'assurer que ces recommandations ne risquent pas de créer des distorsions de concurrence entre les univers mobile et web et/ou d'engendrer des barrières supplémentaires à l'entrée ou à l'expansion dans l'environnement applicatif mobile.

SOMMAIRE

Introduction

1. Le 22 mars 2023, la Commission Nationale de l'Informatique et des Libertés (ci-après, « CNIL ») a saisi l'Autorité de la concurrence (ci-après, « l'Autorité ») sur le fondement de l'article 15 de la loi n° 2017-55 du 20 janvier 2017 portant statut général des autorités administratives indépendantes et des autorités publiques indépendantes. Cet article dispose qu'une « *autorité administrative indépendante ou une autorité publique indépendante peut saisir pour avis une autre autorité de toute question relevant de la compétence de celle-ci* ».

2. Il s'agit de la première saisine pour avis de l'Autorité par la CNIL.

3. Dans sa saisine, la CNIL rappelle que son plan stratégique 2022-2024 comporte, parmi ses priorités, « *des travaux sur les données personnelles dans les applications mobiles* »[3]. Son objectif est de « *mieux comprendre le rôle des données dans l'écosystème mobile, d'apporter des éclairages de doctrine et de la sécurité juridique aux nombreux acteurs de cet écosystème dans leur application des textes relatifs à la protection des données, puis ensuite de mettre en œuvre un plan de contrôle permettant de s'assurer d'un niveau de conformité suffisant de ces acteurs* ».

4. Dans le cadre de ce plan d'action, la CNIL envisage de publier, après plusieurs rencontres avec différents acteurs représentatifs de l'écosystème, une recommandation relative aux applications mobiles, comportant des éléments juridiques et des bonnes pratiques d'ordre technique. La présente saisine de l'Autorité porte sur ce projet de recommandations (ci-après, le « projet »).

5. En janvier 2023, afin de mieux comprendre le fonctionnement du secteur, la CNIL a lancé un appel à contributions concernant les enjeux économiques des données dans l'écosystème mobile[4].

6. Le 21 juillet 2023, la CNIL a publié pour consultation publique et adressé à l'Autorité son projet[5]. La consultation publique de la CNIL sur ce projet a pris fin le 8 octobre 2023.

7. Dans le cadre de l'instruction du présent avis, l'Autorité a sollicité de nombreux acteurs représentant les différents maillons de la chaîne de valeur des applications mobiles (éditeurs, développeurs, fournisseurs de kits de développements logiciels, fournisseurs de magasins d'applications, fournisseurs de systèmes d'exploitation, agences media). Au total, une vingtaine d'acteurs ont été entendus ou ont répondu à des questionnaires.

[3] Lettre de saisine de la CNIL du 22 mars 2023.

[4] https://www.cnil.fr/fr/cloturee-collecte-de-donnees-dans-les-applications-mobiles-la-cnil-lance-une-consultation-publique.

[5] La consultation publique de la CNIL ainsi que le projet de recommandation sur les applications mobiles sont accessibles à ce lien : https://www.cnil.fr/fr/applications-mobiles-la-cnil-lance-une-consultation-publique-sur-son-projet-de-recommandation.

I. Contexte et enjeux relatifs aux applications mobiles

8. Le projet de la CNIL vise notamment à clarifier les obligations des différents acteurs actifs dans le secteur des applications mobiles. Avant d'exposer ces obligations (C), et la réglementation applicable en matière de protection de données personnelles (B), l'Autorité s'attachera à présenter le secteur (A).

A. PRESENTATION DU SECTEUR

9. Les applications mobiles sont définies par la CNIL comme des « *logiciels applicatifs distribués dans l'environnement des téléphones mobiles multifonctions (ou smartphones) et tablettes, c'est-à-dire des terminaux individuels et portatifs, permettant un accès au réseau Internet ainsi que, le plus souvent, au réseau téléphonique, et pouvant permettre l'installation et l'exécution d'applications tierces en leur sein* »[6]. Elles constituent l'un des principaux moyens d'accès à des contenus et des services numériques à partir d'un téléphone mobile. Elles permettent d'ajouter des fonctionnalités ou services supplémentaires au terminal mobile dans des domaines très divers (services de réseaux sociaux, de divertissement, d'achats à distance, mobilité, services bancaires, etc.).

10. De multiples acteurs interviennent aux différents maillons de la chaîne de valeur des applications mobiles, depuis leur conception jusqu'à leur distribution auprès des utilisateurs (1). Sur le plan concurrentiel, le secteur des applications mobiles se caractérise par la présence de plateformes verticalement intégrées (2).

1. L'ORGANISATION DU SECTEUR

11. Les cinq grandes catégories d'acteurs visés par le projet de la CNIL sont les fournisseurs de systèmes d'exploitation, les fournisseurs de magasins d'applications, les éditeurs et les développeurs d'applications ainsi que les éditeurs de kits de développements logiciels (« *software development kits* » ou SDK)[7]. Le plus souvent, ces acteurs sont interdépendants.

12. *L'éditeur de l'application* met l'application à la disposition des utilisateurs (le plus souvent par l'intermédiaire d'un ou plusieurs magasins d'applications) pour proposer ses produits ou services. Il en définit également le modèle économique et notamment son mode de financement.

13. L'éditeur de l'application peut procéder lui-même au développement de son application ou la faire développer par un développeur externe.

14. Dans ce second cas, *le développeur* effectue la réalisation technique de l'application pour le compte de l'éditeur sur la base d'un cahier des charges fourni par ce dernier. À ce titre, le développeur conçoit le code de l'application et effectue des choix concernant son architecture tels que ses modalités d'hébergement.

---

[6] Projet de recommandation de la CNIL relative aux applications mobiles, section 2.2 page 5.

[7] Projet de recommandation de la CNIL relative aux applications mobiles, section 2.3 page 6.

15. Pour qu'un utilisateur puisse faire fonctionner son application, celle-ci doit s'exécuter sur le terminal mobile grâce à son système d'exploitation (ci-après, « OS » pour « *operating system* ») spécialement configuré et installé sur le téléphone mobile ou la tablette de l'utilisateur. La CNIL indique que les applications sont le plus souvent exécutées sur le terminal de manière isolée entre elles (modèle de « bac à sable »[8], ou « *sandbox* ») par un système d'exploitation qui limite les ressources OS auxquelles elles peuvent accéder (c'est-à-dire ses capteurs, tel que l'appareil photo ou le GPS, ses fonctionnalités spécifiques, telles que l'accès réseau ou le Bluetooth, ou encore son stockage, tel que la liste des contacts ou la galerie photos) *via* un système de permissions. Les applications peuvent en effet accéder à un certain nombre de fonctionnalités et de données du système *via* des interfaces de programmation applicatives ou API (pour « *application programming interface* »)[9] mises à disposition à cet effet par le fournisseur du système d'exploitation[10]. L'OS définit et assiste l'ensemble des interactions autorisées entre l'utilisateur et le terminal, mais également entre les applications mobiles tierces (celles qui seront installées ensuite) et le terminal.

16. Certaines applications mobiles, dites « natives », sont créées pour un système d'exploitation spécifique. D'autres applications mobiles sont développées pour fonctionner *via* un navigateur Internet et ne sont donc pas spécifiques à un système d'exploitation ; il s'agit des applications « web »[11].

17. Le *fournisseur du système d'exploitation* met à disposition le système d'exploitation spécialement configuré et installé sur le terminal mobile de l'utilisateur, environnement dans lequel l'application sera par la suite exécutée.

18. Les deux principaux systèmes d'exploitation pour téléphones mobiles sont ceux d'Apple (iOS) et de Google (Android). Selon une étude de Kantar de juin 2023, en France près de 74 % des terminaux mobiles auraient un système d'exploitation Android et 26 % un système d'exploitation iOS[12], le système iOS étant exclusivement disponible sur les appareils Apple.

19. Le système d'exploitation d'Android est un système d'exploitation sous licence, ouvert aux fabricants d'appareils mobiles tiers, alors que ces derniers ne peuvent pas obtenir d'Apple la licence iOS pour utiliser ce système d'exploitation sur leurs propres appareils[13].

20. *Les fournisseurs de SDK* offrent un ensemble d'outils utilisés pour le développement de l'application, en fonction du système d'exploitation utilisé. Le recours à des SDK, très fréquent, est notamment dû au fait que ceux-ci permettent le plus souvent de faciliter ou

---

[8] L'exécution en mode « bac à sable » ou « *sandboxing* » est un mécanisme de sécurité mis en œuvre par un système d'exploitation pour isoler une application exécutée vis-à-vis du cœur du système d'exploitation mais aussi des autres applications exécutées sur le terminal. Cette isolation permet de réduire le risque qui pourrait être lié à l'abus de fonctionnalités du terminal, mais aussi à des tentatives d'une application pour accéder à des données ou perturber le fonctionnement d'une application tierce. En général, les applications s'exécutant en mode « bac à sable » ont des fonctionnalités par défaut assez réduites, n'ayant la possibilité d'utiliser que des API fournies par l'OS, sous réserve de l'obtention d'une permission de l'utilisateur.

[9] Une API est une interface logicielle qui permet de mettre en relation un logiciel ou un service à un autre logiciel ou service afin d'échanger des données et des fonctionnalités. Dans le contexte des applications mobiles, les API sont également le moyen par lequel le système d'exploitation propose tout un ensemble de fonctionnalités aux applications.

[10] Projet de recommandation de la CNIL, dispositions relatives aux applications mobiles, section 2.2 page 5.

[11] CMA, "*Mobile ecosystems – Market study final report"*, 10 juin 2022 (page 11, paragraphes 2.6 et 2.7)

[12] Kantar, https://www.kantarworldpanel.com/fr/smartphone-os-market-share/, juin 2023.

[13] Décision de la Commission européenne Google Android en date du 18 juillet 2018, n° 40099, paragraphes de 238 à 241.

d'accélérer le développement de fonctionnalités logicielles, en évitant au développeur d'écrire l'intégralité du code de l'application. En pratique, il s'agit d'une brique logicielle tierce implantée dans l'application permettant, à l'instar du code écrit par le développeur lui-même, de procéder à différentes opérations. Si le SDK peut permettre de réaliser des opérations localement sur le terminal, dans de nombreux cas, les SDK permettent « d'appeler » des fonctionnalités offertes par des services en ligne tiers. Le SDK peut ainsi permettre de mettre en œuvre certaines fonctionnalités dans l'application (par exemple paiement, partage sur les réseaux sociaux, etc.). D'autres SDK permettent d'effectuer des demandes d'accès au système d'exploitation, telles que, par exemple, la géolocalisation permettant le suivi de l'utilisateur de l'application à différentes fins (marketing, publicité, etc.).

21. Une fois réalisées, les applications sont distribuées auprès des utilisateurs, principalement par l'intermédiaire d'un ou plusieurs magasins d'applications. Certaines applications peuvent toutefois être déjà préinstallées sur le terminal de l'utilisateur ou, de façon marginale, être téléchargées directement depuis Internet (*i.e.* « *sideloading* »).

22. *Le fournisseur de magasins d'applications* met à disposition une plateforme de distribution en ligne des applications, sous la forme d'une application accessible sur le terminal de l'utilisateur depuis un système d'exploitation compatible (par exemple l'App Store pour un terminal doté du système d'exploitation iOS d'Apple, ou le Play Store pour un terminal doté du système d'exploitation Android de Google). Les magasins d'applications mobiles mettent en relation et gèrent les transactions entre d'une part, les utilisateurs de téléphone mobile ou tablette, qui utilisent le magasin pour rechercher et télécharger des applications et d'autre part, les éditeurs, qui offrent leurs applications mobiles. Ce sont des plateformes multi-faces.

23. Le fournisseur du magasin d'applications est fréquemment, mais pas systématiquement, le fournisseur du système d'exploitation. Un magasin d'applications spécifique peut aussi être fourni par le constructeur du terminal (Samsung, Huawei, etc.). Pour le système d'exploitation Android, des magasins d'applications alternatifs proposés par des tiers non-constructeurs, dont l'utilisation reste marginale, peuvent en principe être installés en tant qu'applications standards (F-Droid, Aurora Store, etc.).

2. LES ENJEUX CONCURRENTIELS

24. La structure concurrentielle du secteur des applications mobiles se caractérise par plusieurs éléments.

25. En premier lieu, ce secteur se distingue par la présence d'acteurs verticalement intégrés tout au long de la chaîne de valeur des applications mobiles.

26. En effet, Alphabet Inc. (ci-après, « Google ») et Apple sont présents à tous les niveaux de la chaîne de valeur. Ces acteurs sont à la fois fournisseurs d'OS, de magasins d'applications et de SDK, éditeurs, développeurs et fournisseurs d'autres services. Ils sont donc concernés par l'ensemble des sections du projet de la CNIL[14].

27. En particulier, outre le développement et l'édition d'applications propriétaires (par exemple Apple Music ou YouTube), ces opérateurs proposent des SDK, dont certains sont très utilisés, voire considérés comme incontournables par certains développeurs ou éditeurs tiers

[14] Par ailleurs, Apple et Google sont également fournisseurs de terminaux (*i.e.* smartphones et tablettes).

pour le développement de leurs propres applications, qu'elles soient au contact de l'utilisateur (« front-end ») ou utilisées en arrière-plan (« back-end », par exemple, le SDK Firebase[15] de Google).

28. S'agissant de la distribution des applications mobiles, Apple et Google distribuent leurs applications propriétaires par l'intermédiaire de leurs propres magasins d'applications, les rendant disponibles au téléchargement au même titre que celles de leurs concurrents[16] ou les préinstallent sur le téléphone ou la tablette de l'utilisateur (directement dans le cas d'Apple et en fonction des accords avec les constructeurs pour les téléphones Android non fabriqués par Google).

29. En deuxième lieu, ces acteurs verticalement intégrés sont susceptibles de détenir une position dominante sur certains marchés de la chaîne de valeur des applications mobiles.

30. À titre d'exemple, dans sa décision de 2018 relative à l'affaire Google Android, la Commission européenne (ci-après, la « Commission ») a conclu que Google détenait depuis 2011 une position dominante sur le marché mondial (à l'exception de la Chine) des systèmes d'exploitation mobiles intelligents sous licence ainsi que sur le marché mondial (à l'exception de la Chine) des boutiques d'applications Android[17]. Le Tribunal de l'Union européenne a confirmé cette analyse[18].

31. Également à titre d'exemple, s'agissant de la position d'Apple sur le marché de la distribution d'applications sur iOS, l'Autorité a considéré, dans une décision de mesures conservatoires qui ne préjuge pas de l'affaire au fond, que « *compte tenu du fait que l'App Store d'Apple constitue le seul canal de distribution des applications mobiles sur les appareils iOS, Apple apparaît susceptible, à ce stade de l'instruction, de détenir une situation de monopole sur ce marché* »[19].

---

[15] Firebase offre aux développeurs une suite d'outils et de services qui permet « [d'accéder] *plus vite au marché avec un back-end sécurisé et entièrement géré, et un processus de développement simplifié qui vous laisse vous concentrer sur l'essentiel* ». https://firebase.google.com.

Elle offre notamment un système d'authentification, un service de cloud (informatique en nuage) pour développer le back-end d'une application sans serveurs, un service de base de données en temps réel, des extensions pour ajouter rapidement des fonctionnalités supplémentaires à partir d'ensembles de codes open source, un ensemble d'outils et de services (Firebase Machine Learning) permettant d'apporter de puissantes fonctionnalités d'apprentissage automatique à l'application etc.

Selon le premier baromètre des SDK du marché français publié par la Mobile Marketing Association France et App Annie en 2019, le SDK Google Firebase était l'un des plus populaires en France en 2019. https://www.mobilemarketing.fr/les-sdk-google-equipent-plus-de-80-des-applications-francaises/.

[16] CMA, "*Mobile ecosystems – Market study final report*", du 10 juin 2022, page 16, paragraphe 2.25.

[17] Décision de la Commission européenne Google Android du 18 juillet 2018, n° 40099, section 9.

[18] Arrêt du Tribunal de l'Union européenne du 14 septembre 2022, Google et Alphabet/Commission (Google Android), affaire T 604/18. Google LLC et Alphabet Inc. ont formé un pourvoi contre cet arrêt (affaire C 738/22 P).

[19] Décision n° 21-D-07 du 17 mars 2021 relative à une demande de mesures conservatoires présentée par les associations Interactive Advertising Bureau France, Mobile Marketing Association France, Union Des Entreprises de Conseil et Achat Media, et Syndicat des Régies Internet dans le secteur de la publicité sur applications mobiles sur iOS, paragraphe 130.

32. En troisième lieu, ces acteurs verticalement intégrés ont mis en place des écosystèmes distincts, dans le cadre desquels ils établissent, en tant que fournisseur d'OS et/ou en tant que fournisseur de magasins d'applications, des règles d'accès spécifiques[20].

33. Sur les terminaux mobiles d'Apple, seul le système d'exploitation iOS est autorisé. La Commission, dans sa décision Google Android, a indiqué qu'il n'était pas possible d'obtenir de licence pour utiliser iOS, car Apple n'accorde pas de licences à des tiers[21]. À date, s'agissant de la distribution des applications mobiles, l'App Store d'Apple constitue le seul canal de distribution des applications mobiles sur les appareils iOS pour les éditeurs, Apple n'autorisant pas le téléchargement d'applications en dehors de son magasin App Store[22].

34. En revanche, si le système d'exploitation Android de Google peut fonctionner sur la plupart des terminaux mobiles hors ceux d'Apple, la Commission a, dans sa décision Google Android précitée, établi l'existence d'un écosystème Android particulier et distinct de celui d'iOS, en indiquant qu'Apple et l'écosystème iOS n'étaient pas en mesure d'exercer une contrainte concurrentielle sur Google et l'écosystème Android susceptible de remettre en question la position dominante de Google sur les marchés pertinents[23].

35. En dernier lieu, ces acteurs verticalement intégrés ont récemment été désignés « *contrôleurs d'accès* » au sens du règlement sur les marchés numériques (« *Digital Markets Act* », ci-après, le « DMA »)[24] par la Commission.

36. Le DMA vise à empêcher les contrôleurs d'accès d'imposer des conditions inéquitables aux entreprises et aux utilisateurs finaux et à garantir l'accessibilité à des services numériques importants. Ce règlement, en vigueur depuis novembre 2022 et appliqué depuis mai 2023, vise à garantir la contestabilité et l'équité des marchés dans le secteur numérique et, partant, à offrir davantage de choix et de liberté aux utilisateurs finaux et aux entreprises utilisatrices des services des contrôleurs d'accès. Il régit certains services des contrôleurs d'accès, à savoir de grandes plateformes en ligne qui constituent un point d'accès majeur entre les entreprises utilisatrices et les consommateurs et qui, de par leur position, peuvent créer un goulet d'étranglement dans l'économie numérique.

37. Le 6 septembre 2023, en application du DMA, Google et Apple ont notamment été désignés contrôleurs d'accès pour plusieurs services de plateforme essentiels, dont : [25]

---

[20] Voir à titre d'exemple en ce sens, CMA, "*Mobile ecosystems – Market study final report*", du 10 juin 2022, page 16, paragraphe 2.25 : « *Apple et Google distribuent également un grand nombre de leurs propres applications par l'intermédiaire de leurs boutiques d'applications, les rendant disponibles au téléchargement à côté de celles de leurs concurrents. En ce sens, ils sont en concurrence sur divers marchés d'applications pour lesquels ils exercent également une puissante fonction de fixation de règles* » (traduction par nos soins, soulignement ajouté).

[21] Décision de la Commission européenne Google Android du 18 juillet 2018, n° 40099, paragraphe 239.

[22] Décision n° 21-D-07 précitée, paragraphe 110.

[23] Décision de la Commission européenne Google Android du 18 juillet 2018, n° 40099, paragraphes de 238 à 267.

[24] Règlement (UE) 2022/1925 du Parlement européen et du Conseil du 14 septembre 2022 relatif aux marchés contestables et équitables dans le secteur numérique et modifiant les directives (UE) 2019/1937 et (UE) 2020/1828.

[25] Voir la version non confidentielle des décisions de désignation. Alphabet n'a pas fait appel de la désignation de Google pour ses services essentiels (https://www.reuters.com/technology/microsoft-google-not-challenge-eu-gatekeeper-designation-2023-11-14/). Concernant Apple, seul iOS est actuellement concerné, mais la Commission a ouvert une enquête de marché afin d'examiner si l'iPadOS, bien qu'il n'atteigne pas les seuils

- leurs systèmes d'exploitation pour terminaux mobiles respectifs (Google Android et iOS) ;
- leurs services d'intermédiation de magasins d'applications respectifs (Google Play Store et App Store).

38. Après leur désignation, les contrôleurs d'accès disposent d'un délai de six mois pour se conformer à la liste complète des obligations et interdictions prévues par le DMA. Toutefois, certaines des obligations commencent à s'appliquer dès la désignation, par exemple l'obligation d'informer la Commission de toute concentration envisagée. La Commission est chargée du contrôle du respect de ces obligations[26].

39. Si les contrôleurs d'accès ne détiennent pas nécessairement de position dominante au sens du droit de la concurrence[27], le fait que certaines entreprises soient désignées comme tels est l'un des éléments à prendre en compte lors de l'examen de leur pouvoir de marché dans un marché déterminé.

40. Par ailleurs, les enjeux concurrentiels dans le secteur des applications mobiles ont également fait l'objet de rapports élaborés par plusieurs autorités nationales de concurrence ou institutions, lesquelles ont identifié des préoccupations de concurrence[28].

41. Par exemple, le 10 juin 2022, la *Competition and Markets Authority* du Royaume-Uni (ci-après, la « CMA ») a publié un rapport final relatif à son étude de marché sur les écosystèmes mobiles, dans lequel elle expose ses conclusions et ses préoccupations ainsi que des remèdes potentiels[29].

42. Dans son rapport, la CMA indique qu'Apple et Google contrôleraient des points d'accès clés de plus en plus cruciaux (*i.e.* systèmes d'exploitation, magasins d'applications et navigateurs web), ce qui les placerait en position de force. Ces deux entreprises détermineraient unilatéralement les « règles du jeu », compliquant ainsi la tâche des entreprises concurrentes, comme par exemple les navigateurs ou les autres magasins d'applications[30].

43. Le 9 février 2023, la *Japan Fair Trade Commission* (ci-après, la « JFTC») a également publié une étude de marché sur les systèmes d'exploitation mobiles et la distribution des

---

de désignation, devrait être désigné comme service essentiel. Apple a toutefois fait appel devant le Tribunal de l'Union européenne de la désignation d'iOS et AppStore comme services essentiels (cas T1080/23).

[26] Il appartient aux entreprises désignées de veiller au respect effectif des règles et d'en faire la démonstration. À cet effet, elles disposent d'un délai de six mois pour présenter un rapport de conformité détaillé décrivant la manière dont elles respectent chacune des obligations du règlement sur les marchés numériques.

Si un contrôleur d'accès ne respecte pas les obligations fixées par le règlement sur les marchés numériques, la Commission peut lui infliger des amendes allant jusqu'à 10 % du chiffre d'affaires mondial total de l'entreprise, et jusqu'à 20 % en cas d'infraction répétée. En cas d'infraction systématique, la Commission a également le pouvoir d'adopter des mesures correctives supplémentaires, telles qu'obliger un contrôleur d'accès à vendre tout ou partie d'une activité ou lui interdire d'acquérir des services supplémentaires en rapport avec l'infraction systémique.

[27] DMA, considérant n° 5.

[28] CMA, "*Mobile ecosystems – Market study final report*", du 10 juin 2022 ; Japan Fair Trade Commission, "*Market study report on mobile OS and mobile app distribution*", février 2023 ; US Department of Commerce "*Competition in the mobile application ecosystem"*, février 2023

[29] https://www.gov.uk/government/publications/mobile-ecosystems-market-study-final-report.

[30] « *CMA's market study into mobile ecosystems: final report summary*", page 1, https://assets.publishing.service.gov.uk/media/62a228228fa8f50395c0a104/Final_report_summary_doc.pdf.

applications mobiles[31]. Dans l'analyse relative aux fournisseurs de systèmes d'exploitation mobiles et aux magasins d'applications (page 14), la JFTC indique notamment que les consommateurs japonais n'ont le choix qu'entre deux écosystèmes mobiles, respectivement centrés sur Android et sur iOS. Le rapport (page 25) relève que si, en général, l'intégration verticale des services liés sur différents maillons (*i.e.* intégration verticale) peut améliorer l'efficacité et le confort du consommateur, les entreprises verticalement intégrées peuvent être tentées d'accorder un traitement préférentiel à leurs produits et services connexes, ce qui pourrait entraîner une baisse de la qualité et une hausse des prix des produits et services.

B. LA REGLEMENTATION APPLICABLE A LA PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL

44. Les multiples acteurs qui interviennent dans le secteur des applications mobiles sont soumis à la réglementation relative à la protection des données personnelles lorsque, par l'intermédiaire d'une application :

- des opérations de lecture et d'écriture, telles que définies par l'article 82 de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (ci-après, la « loi Informatique et Libertés »)[32], en application de la directive « vie privée et communications électroniques », (ci-après, la « directive e-Privacy »[33]), qu'elles portent ou non sur des données personnelles, sont effectuées sur le terminal mobile ;
- des opérations constituent un traitement de données personnelles au sens de l'article 4 du Règlement général sur la protection des données (ci-après, le « RGPD »)[34].

45. Les manquements au RGPD et aux mesures de droit national transposant la directive e-Privacy[35] sont passibles de sanctions importantes (jusqu'à 20 millions d'euros ou, dans le cas d'une entreprise jusqu'à 4 % du chiffre d'affaires annuel mondial).

---

[31] https://www.jftc.go.jp/en/pressreleases/yearly-2023/February/230209.html.

[32] La loi n° 2018-493 du 20 juin 2018, promulguée le 21 juin 2018, a modifié la loi Informatique et Libertés afin de mettre en conformité le droit national avec le cadre juridique européen. Elle permet la mise en œuvre concrète du Règlement général sur la protection des données et de la Directive « police-justice », applicable aux fichiers de la sphère pénale.

[33] Directive 2002/58/CE du Parlement européen et du Conseil concernant le traitement des données à caractère personnel et la protection de la privée dans le secteur des communications électroniques, 12 juillet 2002.

[34] Règlement UE 2016/679 du Parlement européen et du Conseil 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 direction 95/46/CE, 27 avril 2016.

[35] À titre d'exemple, l'article 82 de la loi Informatique et Libertés transpose en droit français l'article 5.3 de la directive e-Privacy. La loi pour la confiance dans l'économie numérique (LCEN) du 21 juin 2004 a également contribué à la transposition de la directive 2002/58, pour ce qui concerne le consentement du destinataire d'une publicité (principe de « l'opt-in » consistant à obtenir l'accord exprès du destinataire de la publicité préalablement à son envoi). La loi du 6 août 2004 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel a achevé le volet législatif de la transposition.

1. LA DIRECTIVE E-PRIVACY

46. La directive e-Privacy, modifiée en 2009, encadre et harmonise les dispositions des États membres en matière de traitement des données dans le secteur des communications électroniques, ainsi que la libre circulation de ces données, des équipements et des services de communications électroniques au sein de l'Union européenne.

47. L'article 82 de la loi Informatique et Libertés telle que modifiée en 2018, qui transpose la directive e-Privacy, s'applique en complément des règles générales du RGPD, dès lors qu'un opérateur accède à des informations déjà stockées dans l'équipement terminal de l'utilisateur par voie de transmission électronique (par exemple, un identifiant publicitaire) ou y inscrit des informations.

48. L'article 5 paragraphe 3 de la directive e-Privacy pose ainsi le principe d'un consentement préalable de l'utilisateur avant le stockage d'informations sur son terminal ou l'accès à des informations déjà stockées sur celui-ci, sauf si ces actions sont strictement nécessaires à la fourniture d'un service de communication en ligne expressément demandé par l'utilisateur ou ont pour finalité exclusive de permettre ou faciliter une communication par voie électronique.

2. LE REGLEMENT GENERAL SUR LA PROTECTION DES DONNEES

49. Le RGPD encadre et harmonise les règles en matière de traitement des données personnelles sur le territoire de l'Union européenne.

50. La loi Informatique et Libertés a été modifiée en 2018 afin d'adapter le droit national au RGPD et à la directive e-Privacy. Le RGPD renforce le contrôle des citoyens sur l'utilisation de leurs données.

51. Entré en application le 25 mai 2018, le RGPD s'applique à tous les traitements de données à caractère personnel. Son article 4 définit une donnée à caractère personnel comme toute information se rapportant à une personne physique identifiée ou identifiable. Selon ce même article, est réputée être une « personne physique identifiable » une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale.

52. L'une des pierres angulaires du RGPD est le principe du recueil du consentement[36]. Les responsables du traitement des données doivent recueillir le consentement explicite de l'utilisateur avant tout traitement de ses données à caractère personnel. Ce consentement doit être libre, spécifique, éclairé et univoque. En outre, le RGPD prévoit que l'utilisateur doit être en mesure de retirer ce consentement, à tout moment, avec la même simplicité qu'il l'a accordé.

---

[36] Le consentement est une des bases légales prévues par le RGPD sur laquelle peut se fonder un traitement de données personnelles. Le RGPD impose que ce consentement soit libre, spécifique, éclairé et univoque. Les conditions applicables au consentement sont définies aux articles 4 et 7 du RGPD. La notion de consentement est différente de celle de « permissions d'accès » correspondant en revanche à des dispositifs mis en œuvre par les OS des terminaux mobiles pour permettre aux utilisateurs de choisir quelles fonctionnalités sont accessibles aux applications mobiles.

53. Les traitements de données à caractère personnel recouvrent toutes les opérations portant sur des données personnelles, quel que soit le procédé utilisé (collecte, enregistrement, organisation, conservation, adaptation, modification, extraction, consultation, utilisation, communication par transmission, diffusion ou toute autre forme de mise à disposition, rapprochement)[37].

54. Le RGPD est applicable à tous les responsables de traitement, qu'ils soient privés ou publics, (entreprises, administrations, associations ou autres organismes), et à leurs sous-traitants (hébergeurs, intégrateurs de logiciels, agences de communication, etc.) établis dans l'UE, et ce quel que soit le lieu de traitement des données. Il s'étend également aux responsables de traitement et à leurs sous-traitants établis hors UE lorsque ces acteurs mettent en œuvre des traitements de données personnelles de personnes se trouvant sur le territoire de l'UE liés à l'offre de biens ou de services à ces personnes dans l'UE ou au suivi du comportement, au sein de l'UE, de ces personnes.

55. S'agissant des traitements des données personnelles impliqués dans le contexte des applications mobiles, l'éditeur traite, dans la majorité des cas, des données personnelles à l'occasion de l'utilisation de son application : données techniques de connexion, données fournies par l'utilisateur lui-même ou déjà présentes sur son terminal, données inférées de sa navigation[38]. Il peut ainsi s'agir de toute donnée nécessaire à la fourniture d'un bien ou service au travers de cette application (données de contact, de paiement, de géolocalisation, etc.), comme de données liées au fonctionnement de l'application en elle-même (recueil de données techniques pour assurer le bon fonctionnement de l'application, vérification de la compatibilité de la version de l'OS, etc.). L'éditeur peut également transmettre les données collectées à cette occasion à des tiers, notamment à des fins de monétisation de son audience, *via* différents moyens propres à l'écosystème mobile (mise en place de traceurs spécifiques à l'environnement mobile, mise à disposition de l'identifiant mobile de l'utilisateur, etc.).

56. Le développeur de l'application, en participant au développement, configure de futurs traitements de données personnelles. En participant à sa maintenance, le développeur peut être impliqué dans l'ensemble des traitements de données personnelles réalisés par l'application et parfois endosser une forme de responsabilité au titre du RGPD[39].

57. Les fournisseurs de SDK conçoivent des briques logicielles susceptibles de configurer de futurs traitements de données personnelles. Ils peuvent par ailleurs être impliqués dans différents traitements de données personnelles à travers ces briques logicielles, dépendant des caractéristiques et des finalités de chaque SDK, et parfois endosser une responsabilité au titre du RGPD[40].

58. Le fournisseur d'OS crée et gère des identifiants propres à chaque terminal ou compte utilisateur, qui permettent l'identification de l'utilisateur à différentes fins : finalités

---

[37] Le RGPD ne s'applique toutefois pas aux traitements de données personnelles relevant exclusivement de l'exemption domestique. Selon la CNIL, pour relever de cette exemption, ces traitements doivent être réalisés par une personne physique et respecter les conditions posées par l'article 2.2.c et le considérant 18 du RGPD. Il s'agit d'une part d'activités « personnelles », qui sont souvent propres à l'activité d'un seul individu et effectuées en principe dans un cadre non professionnel ; d'autre part, d'activités « domestiques », qui sont communes à un nombre limité de personnes, dans un cadre familial ou amical. Pour plus de développement, voir pages 11 et 12 du projet de recommandation de la CNIL.

[38] Projet de recommandation de la CNIL relative aux applications mobiles, section 2.3 page 7.

[39] Projet de recommandation de la CNIL relative aux applications mobiles, section 2.3 page 8.

[40] Projet de recommandation de la CNIL relative aux applications mobiles, section 2.3 page 8.

techniques pour le fonctionnement du terminal, traçage publicitaire, etc. Ils peuvent être utilisés pour le propre compte du fournisseur d'OS ou être transmis à des tiers, notamment les éditeurs d'applications. C'est également à travers les possibilités logicielles proposées par le fournisseur du système d'exploitation que l'éditeur d'une application peut avoir accès aux différents capteurs du terminal mobile (appareil photo, microphone, géolocalisation du terminal, accéléromètres, etc.) ainsi qu'aux données stockées sur ce dernier (carnet de contacts, galerie photographique, liste des applications installées, etc.)[41].

59. En ce qui concerne les fournisseurs de magasins d'applications, la fixation des règles relatives à la publication des applications n'implique pas en soi de traitements de données personnelles[42]. En revanche, le magasin d'applications peut être amené à traiter des données pour ses propres finalités, à l'instar des autres applications mobiles. En particulier, les magasins d'applications sont généralement liés à un compte utilisateur, permettant au moins d'installer les mises à jour des applications.

C. OBJECTIFS ET PRINCIPALES RECOMMANDATIONS DE LA CNIL RELATIVES AUX APPLICATIONS MOBILES

60. La CNIL a inscrit la thématique des applications mobiles comme l'un des axes prioritaires de son programme de travail pour l'année 2023.

61. Comme elle l'indique dans sa consultation publique, l'utilisation d'applications mobiles permet le traitement de grandes quantités de données personnelles. Ces traitements sont mis en œuvre par de nombreux acteurs participant au développement et à la mise à disposition d'une application mobile auprès du public.

62. La CNIL a souhaité apporter davantage de sécurité juridique dans ce domaine, clarifier les qualifications et responsabilités de ces acteurs au regard de la réglementation applicable en matière de protection des données, et rappeler les principes et obligations qui s'appliquent aux traitements de données par les applications mobiles.

63. Afin de construire son projet, la CNIL a conduit une concertation avec différents acteurs représentatifs de l'écosystème des applications mobiles, permettant de mieux comprendre ce secteur : éditeurs d'applications, développeurs, fournisseurs de SDK, fournisseurs d'OS et/ou de magasins d'applications, acteurs institutionnels ainsi que plusieurs représentants de la société civile.

1. LES OBJECTIFS POURSUIVIS PAR LE PROJET DE LA CNIL

64. Dans son projet[43], la CNIL indique que, si les principes et obligations en matière de protection des données sont désormais bien connus des opérateurs de sites web et font déjà l'objet de recommandations, leur mise en œuvre dans le contexte des applications mobiles serait parfois incertaine. Dans ce contexte, le projet vise tout d'abord à clarifier ces règles afin que les acteurs aient une bonne compréhension de leurs obligations au titre de la

[41] Projet de recommandation de la CNIL relative aux applications mobiles, section 2.3 page 6.

[42] Projet de recommandation de la CNIL relative aux applications mobiles, section 2.3 page 7.

[43] Projet de recommandation de la CNIL relative aux applications mobiles, page 4.

réglementation applicable en matière de protection des données ainsi que des bonnes pratiques à mettre en œuvre pour faciliter leur mise en conformité. Ainsi, chaque recommandation thématique de la CNIL rappelle en premier lieu, les principales obligations issues du RGPD et de la loi Informatique et Libertés et édicte, en second lieu, une série de conseils et de bonnes pratiques dont elle préconise la mise œuvre.

65. Dans le cadre du processus de consultation, la CNIL a précisé les quatre grands objectifs que poursuit son projet[44].

66. En premier lieu, le projet vise à préciser le partage des responsabilités entre les différents acteurs constituant l'écosystème mobile ainsi que leurs obligations respectives, en réponse à une demande forte d'acteurs de la chaîne de valeur. Il fournit notamment des outils pour clarifier et encadrer les relations qui peuvent lier ces entités, et en particulier les éditeurs, développeurs et fournisseurs de SDK. Le projet a notamment pour objectif de permettre à chaque acteur d'identifier, pour chaque traitement de données personnelles s'il est, au sens du RGPD, responsable[45] ou co-responsable de traitement, sous-traitant[46] ou s'il ne relève d'aucune de ces qualifications.

67. En deuxième lieu, le projet vise à assurer une information et un recueil du consentement respectueux des utilisateurs. Dans un certain nombre de cas, la collecte et l'utilisation des données personnelles de l'utilisateur nécessitent le recueil de son consentement. En particulier, un certain nombre d'identifiants proposés par l'environnement mobile pour permettre le profilage[47] des utilisateurs ne peuvent être utilisés sans consentement préalable. Le projet vise à clarifier et améliorer la gestion du recueil du consentement des utilisateurs, autant pour encourager la transparence que pour assurer la conformité juridique des professionnels concernés.

68. La CNIL recommande également une articulation entre les demandes de permissions[48] effectuées par les applications pour permettre d'accéder à certaines fonctionnalités et le recueil d'un consentement valable.

---

[44] Pour plus de développement sur les objectifs poursuivis par la CNIL, se référer à la présentation de sa consultation publique.

[45] Le responsable de traitement est la personne morale (entreprise, commune, etc.) ou physique qui détermine les finalités et les moyens d'un traitement, c'est-à-dire l'objectif et la façon de le réaliser. En pratique et en général, il s'agit de la personne morale représentée par son représentant légal.

[46] Le sous-traitant est la personne physique ou morale (entreprise ou organisme public) qui traite des données pour le compte d'un autre organisme (*i.e.* le responsable de traitement), dans le cadre d'un service ou d'une prestation. Les sous-traitants ont des obligations concernant les données personnelles, qui doivent être présentes dans le contrat.

[47] Le profilage est défini à l'article 4 du RGPD. Il s'agit d'un traitement utilisant les données personnelles d'un individu en vue d'analyser et de prédire son comportement, comme par exemple déterminer ses performances au travail, sa situation financière, sa santé, ses préférences, ses habitudes de vie, etc. Un traitement de profilage repose sur l'établissement d'un profil individualisé, concernant une personne en particulier : il vise à évaluer certains de ses aspects personnels, en vue d'émettre un jugement ou de tirer des conclusions sur elle.

[48] Comme indiqué *supra*, à la différence du consentement, qui est une des bases légales prévues par le RGPD sur laquelle peut se fonder un traitement de données personnelles, les permissions d'accès sont des dispositifs mis en œuvre par les OS des terminaux mobiles pour permettre aux utilisateurs de choisir quelles fonctionnalités sont accessibles aux applications mobiles étant donné que ces dernières n'ont par défaut qu'un accès limité à ces fonctionnalités (pour des raisons de sécurité et de protection de la vie privée). L'OS met dès lors à leur disposition des API leur permettant d'effectuer des requêtes afin de se voir autoriser des fonctionnalités additionnelles, sous réserve que l'utilisateur, via une interface fournie par l'OS, l'accepte.

69. En troisième lieu, le projet vise à favoriser des bonnes pratiques, au bénéfice des utilisateurs. En particulier, ce projet ambitionne d'encourager les fournisseurs d'OS et les fournisseurs de magasins d'applications à mettre en œuvre un ensemble de bonnes pratiques pour concourir à un environnement plus respectueux de la protection des données personnelles (amélioration de la qualité et de la fiabilité de l'information présentée à l'utilisateur, finesse du contrôle qu'il peut exercer sur les traitements issus des applications, etc.).

70. Le projet vise enfin à encourager la mise en œuvre d'architectures dans lesquelles les applications mobiles sont de simples logiciels qui fonctionnent hors connexion, sans collecte ou traitement de données personnelles.

2. PRESENTATION DE LA STRUCTURE DU PROJET ET DES PRINCIPALES RECOMMANDATIONS DE LA CNIL

71. Le projet de la CNIL s'adresse aux différentes catégories d'acteurs intervenant dans l'écosystème des applications mobiles.

72. Au sein des catégories, le projet s'adresse plus particulièrement aux délégués à la protection des données[49] et aux équipes techniques et juridiques.

73. Le projet est structuré ainsi :

- les parties 1 et 2 introduisent le document et définissent son périmètre ;
- la partie 3 rappelle les conditions d'application de la réglementation relative à la protection des données à caractère personnel aux applications mobiles ;
- la partie 4 analyse les partages des rôles et des responsabilités des différents acteurs dans la fourniture d'une application mobile au sens du Règlement général sur la protection des données (RGPD), et
- les parties 5 à 9 regroupent les recommandations pratiques et ciblées pour chacune des cinq catégories d'acteurs concernées.

74. S'agissant des éditeurs d'applications (partie 5), la CNIL propose des recommandations concernant la conception de l'application, la cartographie des partenaires, la gestion du consentement et des droits des personnes, le maintien de la conformité durant le cycle de vie de l'application ainsi que concernant les permissions et la protection des données dès la conception.

75. S'agissant des développeurs (partie 6), la CNIL propose des recommandations concernant la relation avec l'éditeur, le rôle de conseil envers l'éditeur, l'usage des SDK ainsi que concernant la sécurité de l'application.

76. S'agissant des fournisseurs de SDK (partie 7), la CNIL propose des recommandations concernant la conception du service, la documentation des bonnes informations, la gestion

[49] Le délégué à la protection des données est chargé de mettre en œuvre la conformité au RGPD au sein de l'organisme qui l'a désigné, s'agissant de l'ensemble des traitements mis en œuvre par cet organisme. Sa désignation est obligatoire dans certains cas. Un délégué, interne ou externe, peut être désigné pour plusieurs organismes sous conditions. Pour garantir l'effectivité de ses missions, le délégué doit disposer de qualités professionnelles et de connaissances spécifiques et doit bénéficier de moyens matériels et organisationnels, des ressources et du positionnement adéquats. (Source : https://www.cnil.fr/fr/definition/delegue-la-protection-des-donnees-dpo).

du consentement et des droits des personnes, ainsi que la participation au maintien de la conformité de l'application au cours du temps.

77. S'agissant des fournisseurs d'OS (partie 8), la CNIL propose des recommandations concernant la conformité des traitements de données personnelles mis en œuvre, la bonne information des partenaires, la fourniture des outils pour permettre le respect des droits et du consentement des utilisateurs ainsi que la fourniture d'une plateforme sécurisée.

78. S'agissant enfin des fournisseurs de magasins d'applications (partie 9), la CNIL propose des recommandations concernant l'analyse des applications soumises par les éditeurs, la mise en œuvre de processus transparents de revue des applications qui intègrent la vérification des règles élémentaires de protection des données, ainsi que l'information des utilisateurs et la fourniture à ceux-ci des outils de signalement et d'exercice des droits.

II. Analyse concurrentielle

79. L'Autorité et la CNIL partagent une ambition commune de protection des données personnelles et de la vie privée (ci-après, « protection de la vie privée ») et du respect de la concurrence.

80. Si la politique de la protection de la vie privée vise à protéger les utilisateurs contre toute collecte et exploitation préjudiciables de leurs données, la politique de la concurrence vise à garantir les conditions d'une concurrence libre et non faussée entre les entreprises sur les marchés dans l'intérêt ultime des consommateurs, en favorisant l'innovation, la diversité de l'offre et des prix attractifs.

81. Malgré ces objectifs distincts, ces deux politiques présentent une certaine convergence d'objectifs, en ce qu'elles sont, *in fine*, mises en œuvre au bénéfice des usagers.

82. Cependant, les interactions entre concurrence et protection de la vie privée peuvent être sources de synergies mais également de tensions.

83. Ainsi, la collecte et l'utilisation des données personnelles peuvent être analysées par les autorités de concurrence selon les trois axes.

84. Tout d'abord, l'accumulation de données contribue à l'établissement du pouvoir de marché des entreprises considérées et appelle en ce sens une vigilance particulière des autorités de concurrence.

85. En outre, le niveau de protection des données des utilisateurs peut constituer un véritable paramètre de concurrence, à l'instar du prix, a fortiori s'il dépasse le niveau imposé par la réglementation sur la protection des données personnelles.

86. Néanmoins, les règles de protection des données ou la manière dont les opérateurs les mettent en œuvre peuvent comporter des risques pour la concurrence, qu'il convient d'identifier et de minimiser. À cet égard, les dispositions du RGPD sont le fruit d'une mise en balance entre plusieurs intérêts légitimes : en premier chef, la protection de la vie privée des utilisateurs, mais également le respect des règles de concurrence. Le législateur a ainsi réalisé cet arbitrage et choisi à travers le RGPD à quel niveau de protection de la vie privée placer le curseur sans affecter trop excessivement l'efficacité des marchés.

87. Des mesures de protection de la vie privée qui iraient au-delà de ce qui est strictement imposé par le RGPD ne sont pas illicites en soi. Toutefois afin d'éviter qu'elles ne nuisent à la bonne efficacité économique des marchés, il est essentiel qu'elles soient définies et mises en œuvre en évitant d'engendrer des effets anticoncurrentiels qui ne seraient pas contrebalancés par un gain suffisant pour les consommateurs. Ceci est particulièrement important lorsque de telles mesures sont mises en œuvre par des opérateurs dominants qui doivent alors veiller à s'assurer que ces règles soient proportionnées et appliquées de manière objective, transparente et non discriminatoire.

88. Après avoir exposé les conditions dans lesquelles la concurrence peut s'exercer sur le paramètre de la protection des données personnelles (A), l'Autorité s'attachera à mettre en évidence les interactions entre la protection de la vie privée et la politique de concurrence (B). Compte tenu de ces éléments, le présent avis analyse ensuite le projet de la CNIL et, notamment, identifie des dispositions plus particulièrement susceptibles de soulever des problématiques du point de vue du droit de la concurrence (C).

A. LA PROTECTION DES DONNEES PERSONNELLES ET DE LA VIE PRIVEE COMME PARAMETRE DE LA CONCURRENCE

89. La pratique décisionnelle reconnaît que la protection de la vie privée peut être un paramètre de concurrence (1). Si la littérature économique et sociale relève que la concurrence sur ce paramètre s'exerce dans des conditions particulières, elle identifie des leviers sur lesquels les régulateurs peuvent agir (2).

1. LA PROTECTION DE LA VIE PRIVEE, UN PARAMETRE DE CONCURRENCE PRIS EN COMPTE DANS LA PRATIQUE DECISIONNELLE

90. L'augmentation des préoccupations des utilisateurs s'agissant de la collecte et de l'utilisation de leurs données personnelles est largement documentée, ainsi que l'adoption par ces derniers d'un comportement visant à améliorer la confidentialité de leurs informations[50]. Plusieurs études montrent en outre que, dans certaines conditions (par exemple, une transparence de l'information s'agissant de la politique de confidentialité), (i) les utilisateurs tendent à opter, toutes choses égales par ailleurs, pour le service offrant une meilleure protection des données personnelles ; et (ii) la disposition à payer des utilisateurs augmente avec le niveau de protection des données personnelles[51].

---

[50] Par exemple, voir : IFOP en partenariat avec la CNIL, 2020, les français et la réglementation en matière de cookies. Commission européenne, 2016, Flash Eurobarometer 443 – Report e-Privacy. Hoofnagle, Chris Jay and Urban, Jennifer M., 2014, "Alan Westin's Privacy Homo Economicus", *Wake Forest Law Review* 49(261); Rainie, Lee, Sara Kiesler, Ruogu Kang, and Mary Madden., 2013, "Anonymity, Privacy, and Security Online." *Washington, DC: Pew Research Center*.

[51] Par exemple, voir : Tsai, Janice Y., Egelman, Serge, Cranor, Lorrie and Acquisti, Alessandro, 2011, "The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study", *Information Systems Research*, 22(2), 254-268 ; Garrett Glasgow and Sarah Butler, 2016, "The value of non-personally identifiable information to consumers of online services: evidence from a discrete choice experiment", *Applied Economics Letters*, *24*(*6*), *392-395*.

91. Si les utilisateurs attachent de l'importance à la protection de la vie privée, ce paramètre ne représente cependant qu'un élément d'arbitrage parmi d'autres. Ainsi, ils peuvent être amenés à la considérer comme secondaire par rapport à d'autres caractéristiques des produits (par exemple, le prix ou les fonctionnalités du bien ou service)[52]. Enfin, les préférences des individus en matière de protection de la vie privée sont vraisemblablement hétérogènes[53].

92. Dans la mesure où la protection de la vie privée peut être l'un des paramètres pris en compte par les utilisateurs pour exercer leurs choix de consommation, les entreprises peuvent se faire concurrence en cherchant à se différencier de leurs concurrents sur ce paramètre. L'équilibre concurrentiel résultant des décisions des utilisateurs et des entreprises peut ainsi aboutir à un niveau différencié de protection de la vie privée.

93. Dans ce contexte, en cohérence avec l'importance croissante accordée par les consommateurs à la protection de leur vie privée, la pratique décisionnelle européenne et française a reconnu cet élément comme étant un paramètre de concurrence.

94. À titre d'exemple, la Commission a estimé, dans sa décision de contrôle des concentrations Microsoft/LinkedIn du 6 décembre 2016[54], que la protection de la vie privée constituait un facteur de qualité important sur le marché des réseaux sociaux professionnels – et donc un paramètre de concurrence. Dans sa décision, elle indique notamment :

« *Les questions liées à la protection de la vie privée en tant que telles ne relèvent pas du droit européen de la concurrence, mais peuvent être prises en compte dans le cadre de l'appréciation réalisée sous l'angle de la concurrence, dans la mesure où les consommateurs les considèrent comme un facteur de qualité important et où les parties à la concentration se livrent concurrence sur ce facteur. En l'espèce, la Commission a conclu que la protection de la vie privée constituait un paramètre important de la concurrence entre les réseaux sociaux professionnels existant sur le marché, et que l'opération aurait pu y porter atteinte* »[55].

95. Dans son arrêt Google Android du 14 septembre 2022[56], le Tribunal de l'Union européenne a également estimé, s'agissant des services de recherche générale et de navigation sur

---

[52] À titre illustratif, une expérience a pu être menée au cours de laquelle « *une écrasante majorité des participants acceptaient d'acheter des DVD auprès d'un marchand en ligne assurant un plus faible niveau de protection de la vie privée parce que les prix pratiqués étaient inférieurs* », OCDE, « Droits relatifs aux données des consommateurs et impact sur la concurrence – Note de référence du Secrétariat », 10-12 juin 2020.

D'autres études mettent en évidence la nature profonde des humains, qui seraient avant tout des êtres sociaux aimant créer des contacts, notamment par le partage d'information. Voir par exemple "*Privacy and human behavior in the age of information*", Acquisti, Alessandro and Brandimarte, Laura and Loewenstein, George, Science, 347(6221), 509–514, 2015

[53] Il ressort en effet de la littérature qu'en matière de protection des données personnelles, les préférences des individus sont influencées tant par des facteurs sociaux, culturels, économiques que par l'existence de bénéfices et de préjudices liés à la divulgation d'information, qu'ils soient individuels (e.g. services personnalisés, remises fidélité, coût de recherche réduit, information pertinente) ou collectifs (e.g. révélation d'effets secondaires inattendus pour les médicaments, alerte épidémique, manipulation de masse). Voir, e.g., Stigler Committee on Digital Platforms, Final Report, 2019 et A. Acquisti, C. Taylor and L. Wagman, "The Economics of Privacy", *Journal of Economic Literature* 2016, 54(2), 442–492.

[54] COMP/M.8124 – Microsoft / LinkedIn, 6 décembre 2016.

[55] Communiqué de presse de la Commission européenne relatif à la décision de concentration COMP/M.8124 – Microsoft / LinkedIn, 6 décembre 2016, soulignement ajouté.

[56] Arrêt T-604/18 du 14 septembre 2022 Google Android, point 578, soulignements ajoutés.

internet, que la protection de la vie privée pouvait être un paramètre de choix des consommateurs :

« *En outre, ainsi que cela ressort des pièces du dossier, les besoins des consommateurs ne sont pas nécessairement satisfaits par la solution qualitativement la meilleure, à supposer que Google puisse alléguer que ses services représentent une telle solution, étant donné que d'autres variables que la qualité technique, comme la protection de la vie privée ou la prise en compte des spécificités linguistiques des demandes de recherche effectuées jouent également un rôle.* »[57]

96. L'Autorité s'est également déjà exprimée sur le sujet. Dans un avis rendu le 6 mars 2018[58], portant sur l'exploitation des données dans le secteur de la publicité sur internet, elle a considéré que « [l]*e cadre juridique relatif à la protection des données personnelles et de la vie privée, ainsi que les conditions de mise en œuvre de ces règles par les acteurs sont des paramètres importants du fonctionnement concurrentiel du marché* »[59]. Sur l'importance des données personnelles comme élément de concurrence entre les acteurs, elle a également considéré que « [l]*es données personnelles sont un intrant très particulier dont les possibilités de monétisation sont strictement encadrées par le législateur. Si le ciblage publicitaire ne repose pas uniquement sur les données personnelles, la valeur désormais associée aux possibilités de traitement de ces données en font* [sic] *un élément déterminant de la concurrence que se livrent les acteurs. En ce sens, le respect plus ou moins strict des règles de protection des données personnelles est susceptible de renforcer ou d'affaiblir les positions des acteurs* »[60].

97. Dans sa récente décision relative à une demande de mesures conservatoires dans le secteur de la publicité sur applications mobiles sur iOS, l'Autorité a constaté « [qu']*il apparaît* […] *que cette politique de protection de la vie privée répond à une demande croissante des consommateurs* »[61].

98. Enfin, dans la décision d'engagements de Meta du 16 juin 2022[62], l'Autorité a indiqué que « *la concurrence entre les réseaux sociaux s'exerce à travers une combinaison de paramètres tels que le nombre et les catégories d'utilisateurs, les contenus proposés, les fonctionnalités, la qualité de la publicité, la protection de la vie privée, la gouvernance de la plateforme, le prix* »[63].

---

[57] Soulignements ajoutés.

[58] Avis n° 18-A-03 du 6 mars 2018 portant sur l'exploitation des données dans le secteur de la publicité sur internet.

[59] Avis n° 18-A-03 précité, page 38, soulignements ajoutés.

[60] Avis n° 18-A-03 précité, page 112, soulignement ajouté.

[61] Décision n° 21-D-07 précitée, paragraphe 146.

[62] Décision n° 22-D-12 du 16 juin 2022 relative à des pratiques mises en œuvre dans le secteur de la publicité sur internet, paragraphe 247, soulignement ajouté.

[63] Soulignement ajouté.

2. LA CONCURRENCE SUR CE PARAMETRE S'EXERCE CEPENDANT DANS DES CONDITIONS PARTICULIERES

99. Bien que les consommateurs déclarent fréquemment être opposés à la collecte et au traitement de leurs données personnelles, ces intentions ne transparaissent pas toujours dans leur comportement (phénomène qualifié de « *privacy paradox* »)[64]. Cette différence peut en réalité s'expliquer par le fait que les comportements des consommateurs sont spécifiques et contextuels[65], c'est-à-dire directement liés aux conditions dans lesquelles les consommateurs sont placés au moment de choisir de divulguer ou non une information personnelle, mais également par les caractéristiques mêmes de certains marchés et le comportement des entreprises fournissant les produits et services.

100. En effet, si de plus en plus d'utilisateurs accordent de l'importance à la protection de leur vie privée, la concurrence exercée sur ce critère se heurte à plusieurs caractéristiques spécifiques au secteur numérique, pouvant justifier l'intervention d'autorités de régulation, notamment : la forte concentration de l'offre sur certains marchés autour de grandes plateformes numériques face à une forte atomicité de la demande (a), des facteurs d'altération de la rationalité des utilisateurs tendant à renforcer encore davantage le pouvoir de marché de certains acteurs (b) ainsi qu'un coût social lié à l'exploitation abusive ou à la divulgation de données personnelles pouvant être supérieur à la disposition à payer des utilisateurs pour la protection de leurs données personnelles (c).

a) Structure de marché

101. Plusieurs marchés du secteur du numérique sont caractérisés par une tendance naturelle à la concentration autour de plateformes bénéficiant d'un pouvoir structurant et difficilement contestable.

102. Cette tendance peut s'expliquer par l'existence de fortes économies d'échelle et/ou de gamme et d'externalités de réseau directes et indirectes, lesquelles peuvent rendre ces marchés susceptibles de basculer au profit d'un seul acteur (« *tipping* »)[66] et renforcer par ailleurs les barrières à l'entrée[67].

---

[64] L'une des premières expériences illustrant le « *privacy paradox* » proposait à des participants, préalablement classés selon le niveau de leurs préoccupations en matière de confidentialité, d'acheter des produits à prix réduit avec l'aide d'un agent commercial. Cette étude a mis en évidence que, quel que soit leur niveau de préoccupation pour la confidentialité, peu d'individus ont montré des réticences à répondre aux questions sensibles posées par l'agent.

Spiekermann, J. Grossklags, B. Berendt, E-Privacy in 2nd Generation E-Commerce: Privacy Preferences versus Actual Behavior (Third ACM Conference on Electronic Commerce, Tampa, 2001), pp. 38-47.

[65] A. Acquisti, C. Taylor and L. Wagman, "The Economics of Privacy", *Journal of Economic Literature* 2016, 54(2), 442-492.

[66] Lorsque les externalités de réseau sont très fortes, le marché se concentre jusqu'à ce qu'une seule plateforme subsiste. En effet, dans ces conditions de marché, une plateforme unique peut être plus efficace.

[67] Stigler Committee on Digital Platforms, Final Report, 2019.

103. Les plus grands acteurs de ce marché se sont, par ailleurs, constitués en écosystèmes[68]. Ces environnements qui rassemblent des services intégrés présentent des effets de réseau et des coûts de transfert élevés qui tendent à renforcer le pouvoir de marché de leurs propriétaires.

104. Enfin, les services offerts par ces plateformes étant – dans leur majorité – gratuits pour leurs utilisateurs et pouvant être financés par la publicité ciblée, le rôle des données, le volume de collecte et la possibilité de les combiner sont cruciaux[69], étant relevé que cette collecte intervient sur des marchés sujets aussi à l'intégration verticale de certains acteurs.

105. Ces éléments contribuent au pouvoir de marché d'acteurs importants et bien installés dans ce secteur.

106. Du côté des utilisateurs, l'atomicité de la demande couplée à la complexité croissante des politiques de confidentialité induisent un contrepouvoir de négociation extrêmement faible[70]. Sur certains marchés, les utilisateurs peuvent se trouver captifs d'entreprises en situation de dominance, voire de quasi-monopole. En conséquence, « *les consommateurs ont rarement leur mot à dire en matière de protection de la vie privée en tant que composante de la qualité d'un produit en ligne, dans la mesure où ils n'ont généralement pas la possibilité d'éviter certains fournisseurs de services numériques de premier plan* »[71].

107. Par exemple, la présence d'effets de réseaux importants peut, indépendamment de l'attractivité et de la performance des services offerts, limiter la capacité des consommateurs à fonder leur arbitrage sur le critère de la protection de la vie privée. En effet, les utilisateurs sensibles à la protection de leurs données personnelles peuvent renoncer à opter pour un service plus respectueux de leur vie privée si ce service alternatif ne regroupe pas suffisamment d'utilisateurs ou d'offreurs comparativement au service principal moins respectueux de la vie privée (par exemple, des services de réseaux sociaux, des magasins d'applications). L'émergence d'offres plus protectrices des données personnelles des consommateurs peut en conséquence être freinée par la présence d'entreprises disposant d'un réseau étendu et donc d'un fort pouvoir de marché.

108. Certaines entreprises peuvent alors s'appuyer sur leur position forte dans leurs marchés respectifs pour mettre en œuvre des politiques de collecte et d'utilisation des données peu respectueuses de la vie privée des utilisateurs tant que ces politiques leur sont bénéfiques. À cet égard, dans sa décision du 6 février 2019[72], le Bundeskartellamt a estimé que la position dominante de Facebook sur le marché allemand des réseaux sociaux pour utilisateurs privés plaçait les consommateurs dans une situation de type « à prendre ou à laisser » et que les

---

[68] Les écosystèmes ont été définis comme « *un certain nombre d'entreprises – produisant des biens concurrents ou complémentaires – qui fonctionnent ensemble afin de créer un nouveau marché et de produire des biens et des services ayant une valeur pour les clients* » (Économie numérique : Rapport conjoint de l'Autorité de la concurrence et de la *Competition and Markets Authority* sur l'analyse des systèmes ouverts et fermés, décembre 2014).

[69] Stigler Committee on Digital Platforms, Final Report, 2019.

[70] Stigler Committee on Digital Platforms, Final Report, 2019.

OCDE, « Droits relatifs aux données des consommateurs et impact sur la concurrence – Note de référence du Secrétariat », 10-12 juin 2020.

[71] Robertson, V. (2020), « *Excessive Data Collection: Privacy Considerations and Abuse of Dominance in the Era of Big Data* », Common Market Law Review, vol. 57, pp. 161–189.

[72] Décision du Bundeskartellamt n° B6-22/16 « *Facebook, Exploitative business terms pursuant to Section 19(1) GWB for inadequate data processing* », 6 février 2019.

pratiques de Facebook en matière de données contribuaient à renforcer sa position dominante.

109. Afin de veiller à l'exercice d'une concurrence saine et loyale sur ces marchés, y compris sur la dimension de la protection de la vie privée, les autorités de concurrence ont un rôle de premier plan à jouer en particulier, dans le cadre de leurs missions de contrôle des concentrations, de lutte contre les abus de position dominante et de leurs recommandations visant à améliorer le fonctionnement concurrentiel des marchés (voir section II.B.1).

b) Facteurs d'altération de la rationalité des utilisateurs

110. La littérature en sciences sociales et comportementales identifie plusieurs facteurs d'influence du comportement des utilisateurs en matière de protection de la vie privée[73]. Parmi ces facteurs, l'asymétrie d'information et les biais cognitifs ou comportementaux des utilisateurs peuvent avoir un impact particulièrement important. Si ces facteurs peuvent affecter le bon fonctionnement concurrentiel des marchés et donc nécessiter une réponse des autorités de concurrence, ils peuvent aussi affecter d'autres politiques publiques, notamment la protection de la vie privée (par exemple pour faciliter une meilleure transparence de l'information au bénéfice des utilisateurs) et la protection des consommateurs (par exemple lutter contre certaines pratiques agressives ou trompeuses comme les « dark patterns » [74]).

L'information des utilisateurs

111. Il existe une forte asymétrie d'information entre les utilisateurs de services numériques et les entreprises du secteur. En particulier, le rapport final du comité Stigler[75] indique que, dans la mesure où les utilisateurs sont en relation de façon directe et indirecte avec un nombre croissant d'entreprises, ces derniers ne peuvent étudier chacune des politiques de confidentialité et leurs implications. Plus généralement, les individus ont rarement connaissance du type d'informations collectées, de la façon dont celles-ci sont utilisées ou des conséquences potentielles que cela pourrait engendrer dans le futur[76].

112. Par ailleurs, les utilisateurs peuvent accorder un poids plus important aux avantages immédiats, qu'ils soient immatériels (par exemple, le fait que des amis « aiment » les mises à jour de leur statut en ligne) ou matériels (par exemple, l'obtention d'une réduction

---

[73] Pour une revue de la littérature, voir par exemple « *Privacy and human behavior in the age of information* », Acquisti, Alessandro and Brandimarte, Laura and Loewenstein, George, Science, 347(6221), 509–514, 2015, et les contributions à la table-ronde de l'OCDE « Integrating consumer behaviour insights in competition enforcement », 24 juin 2022, https://www.oecd.org/fr/daf/concurrence/behavioural-insights-in-competition-enforcement.htm.

[74] Un « dark pattern » est une pratique de présentation trompeuse d'une interface utilisateur visant à manipuler ce dernier en tirant parti de biais cognitifs. Ceci peut être par exemple utilisé pour forcer l'individu à partager plus de données que nécessaire ou à accorder plus facilement son consentement ou pour le convaincre de réaliser immédiatement un achat qu'il n'aurait peut-être pas fait (par exemple en faisant croire de façon trompeuse qu'il ne reste que quelques unités du produit en vente).

[75] Stigler Committee on Digital Platforms, Final Report, 2019.

Le comité Stigler est un comité indépendant composé de plus de 30 universitaires, décideurs politiques et experts qui a passé plus d'un an à étudier en profondeur l'impact des plateformes sur l'économie et les lois antitrust, la protection des données, le système politique et l'industrie des médias d'information.

[76] Par exemple, l'utilisation future des données personnelles des utilisateurs ou les possibles failles de sécurité, souvent découvertes a posteriori (Stigler Committee on Digital Platforms, Final Report, 2019, pages 216-217).

commerciale) qu'aux coûts, plus incertains et éloignés, de renoncement à une protection de leurs données personnelles[77].

113. Des études indiquent pourtant que, lorsque l'asymétrie d'information est corrigée (en particulier s'agissant du contenu de la politique de confidentialité et de ses implications), les utilisateurs peuvent effectuer un arbitrage entre gratuité ou qualité du service et protection des données et exprimeraient une préférence pour la confidentialité, même si cela implique une hausse de prix[78].

114. Sur ce point, une meilleure transparence de l'information encouragée par des politiques en faveur de la protection des données personnelles ou par le droit de la consommation, tant sur la collecte et l'utilisation des données personnelles des utilisateurs que sur les moyens pouvant être mis en œuvre afin de protéger leurs données, est de nature à réduire ce biais et permettre un exercice plus libre de la concurrence sur le paramètre de la protection de la vie privée.

Biais cognitifs ou comportementaux des utilisateurs

115. Les entreprises dont la prospérité dépend de la collecte et du traitement de données personnelles ont tiré profit des connaissances en sciences sociales et comportementales afin de promouvoir la divulgation d'informations.

116. Premièrement, certaines interfaces peuvent biaiser le consentement des utilisateurs en instillant une confusion – par exemple, en proposant des boutons de choix dont la conception (taille, couleur) ou le positionnement favorise un choix plutôt qu'un autre, en orientant les utilisateurs – par exemple, en imposant une présélection de choix – ou en les frustrant ou pressant – par exemple en soumettant leur choix à un compte à rebours. Sur ce sujet, une étude du comité Stigler[79] conclut que ces interfaces (ou « dark patterns ») ne permettent pas aux utilisateurs d'exprimer leurs préférences réelles, voire les manipulent pour qu'ils prennent des décisions qui ne correspondent pas à leurs préférences.

117. Si de telles interfaces pourraient provoquer une désaffection des consommateurs, la faible intensité concurrentielle (cf. section II.A.2.a) laisse une certaine latitude aux entreprises qui les utilisent pour recourir à ces stratégies de persuasion très agressives.

---

[77] Les coûts de cette démarche sont souvent incertains et sont généralement supportés à un moment plus éloigné dans le temps (un futur employeur potentiel peut ne pas aimer autant que vos amis l'ont fait à l'époque la photo risquée de vos vacances que vous avez téléchargée ; un commerçant peut collecter des informations sur vous aujourd'hui et les utiliser pour discriminer les prix la prochaine fois que vous vous rendrez dans son magasin).

Voir en particulier A. Acquisti, C. Taylor and L. Wagman, "The Economics of Privacy", *Journal of Economic Literature* 2016, 54(2), 442–492.

Stigler Committee on Digital Platforms, Final Report, 2019.

[78] The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study, Tsai, Janice Y., Egelman, Serge, Cranor, Lorrie and Acquisti, Alessandro, *Information Systems Research*, 22, issue 2, pp. 254-268, 2011. The value of non-personally identifiable information to consumers of online services: evidence from a discrete choice experiment, Garrett Glasgow and Sarah Butler, *Applied Economics Letters*, *24*(*6*), *392--395*, 2016.

[79] Le comité Stigler a conduit une étude afin de quantifier l'impact de ces interfaces sur les choix des consommateurs. Les résultats indiquent que l'utilisation d'un dark pattern modéré augmentait le consentement de +228 % et l'utilisation d'un dark pattern agressif de +371 %. L'étude rassemble un échantillon de 1 762 américains à qui il était demandé de souscrire ou non à une protection contre l'usurpation d'identité (Stigler Committee on Digital Platforms, Final Report, 2019, page 211).

118. Deuxièmement, le paramétrage par défaut peut exercer une forte influence sur la prise de décision, soit parce qu'il peut être perçu comme une recommandation[80], soit parce qu'il nécessite une action de la part de l'individu. Or, un biais en faveur du *statu quo*[81] pousse généralement les consommateurs à valider les paramètres par défaut[82].

119. Ces biais cognitifs ou comportementaux sont susceptibles d'être exploités de façon anticoncurrentielle. Dans l'arrêt Google Android précité, le Tribunal de l'Union européenne a notamment estimé que la pré-installation de services de recherche générale et de navigateurs sur les appareils mobiles intelligents suscitait un « *biais de statu quo* » compte tenu du fait que les utilisateurs avaient tendance à adopter ce qui leur était proposé par défaut[83].

120. S'agissant du choix des individus relatif au niveau de protection de données personnelles souhaité, la politique de concurrence peut ainsi être vigilante à ce que les entreprises ne puissent fausser, à des fins anticoncurrentielles, les arbitrages que les individus peuvent effectuer. De telles pratiques peuvent aussi être abordées sous l'angle de la protection de la vie privée ou de la protection des droits des consommateurs.

c) Les externalités

121. L'appréhension de la protection des données personnelles en tant que paramètre de choix des utilisateurs dans le cadre de leurs décisions de consommation est fondée sur un postulat incomplet qui n'envisage que la dimension privée du bénéfice ou du préjudice causés par les entreprises.

122. Or, les données personnelles sont non-rivales[84] : une fois produites, ces informations peuvent être consommées simultanément par de nombreuses entreprises. Leur caractère éventuellement exclusif[85] dépend de leur environnement juridique et technique[86]. En effet, si elles sont par nature non-exclusives dans la mesure où, une fois diffusées, elles peuvent être partagées avec d'autres agents que l'acteur responsable de leur collecte, il est cependant

---

[80] Recommendations implicit in policy defaults, McKenzie CR, Liersch MJ, Finkelstein SR, *Psychological Science*., 17(5): 414-20, 2006.

[81] Le biais de *statu quo* peut être défini comme la tendance des individus à persister dans leur choix initial, quel qu'il soit. OCDE, « Droits relatifs aux données des consommateurs et impact sur la concurrence – Note de référence du Secrétariat », 10-12 juin 2020.

[82] Par exemple, s'agissant du don d'organes, alors que 85 % des américains déclarent y être favorables, seule une minorité est inscrite sur le registre du don d'organes. En revanche, les pays pour lesquels l'ensemble des citoyens sont présumés donneurs, sauf s'ils sont inscrits dans le registre des refus (par ex. la France), ont un taux de donation bien supérieur.

"Do Defaults Save Lives?", Johnson, Eric J. and Goldstein, Daniel G., *Science*,. 302 :1338-1339, 2003

[83] Arrêt T-604/18 précité.

[84] En économie, la notion de rivalité d'usage entre consommateurs désigne le fait que la consommation d'un bien par un consommateur limite la capacité d'autres consommateurs à consommer le même bien.

[85] La notion d'exclusion renvoie à la capacité de s'accaparer un bien en en payant le prix.

[86] Stigler Committee on Digital Platforms, Final Report, 2019, page 117.

juridiquement et technologiquement possible de les protéger contre la copie ou la fuite (par exemple par le chiffrement)[87].

123. Comme tout bien public (non rival et non exclusif), les données personnelles peuvent engendrer des externalités positives lorsqu'elles sont collectées et traitées. Par exemple, le partage d'imageries médicales peut améliorer la prise en charge des cancers de l'ensemble de la population. Ces gains sociaux ne sont toutefois pas pris en compte par les utilisateurs lorsqu'ils prennent leurs décisions sur la base de leurs préférences individuelles pour la protection de leur vie privée. En outre, l'évolution de l'environnement juridique et technologique relatif à la collecte et au traitement des données personnelles leur a conféré un caractère semi-exclusif limitant de fait les gains sociaux liés au partage de données.

124. La collecte et le traitement des données personnelles peuvent également produire des externalités négatives, engendrant un coût social[88]. À cet égard, les atteintes liées à une mauvaise utilisation des données collectées peuvent être plus importantes que la somme des préjudices privés[89]. Tel peut être le cas, par exemple, lorsque les utilisateurs qui acceptent la collecte de certaines de leurs données personnelles fournissent indirectement des informations sur des tiers qui n'en sont pas informés[90].

125. Si ces coûts et bénéfices sociaux ne sont pas pris en compte par les utilisateurs, leurs décisions peuvent aboutir à un niveau de protection de la vie privée sous-optimal (c'est-à-dire à une sous-protection lorsque les externalités sont globalement négatives et inversement à une surprotection lorsqu'elles sont globalement positives). Ainsi, la présence de cette défaillance de marché liée à l'existence d'externalités non internalisées par les utilisateurs explique en partie la nécessité de développer une régulation de la protection des données personnelles, en tenant compte des conséquences individuelles mais aussi collectives.

B. PROTECTION DE LA VIE PRIVEE ET POLITIQUE DE CONCURRENCE

126. Si la protection de la vie privée et la politique de concurrence ont des objectifs qui convergent (1), dans certaines conditions, la mise en œuvre de règles visant à renforcer la protection de la vie privée (au-delà de ce qui est requis par le RGPD) peut conduire à des tensions avec le champ du droit de la concurrence (2). Dans ce cadre, le récent arrêt Meta du 4 juillet 2023 (ci-après, « l'arrêt Meta ») de la Cour de justice de l'Union européenne (ci-après, la « CJUE »)[91] fournit des précisions quant à la coopération attendue entre autorités nationales de concurrence et autorités de contrôle nationales en matière de protection des données (3).

---

[87] Duch-Brown, N., Martens, B. and Mueller-Langer, F., 2017, "The economics of ownership, access and trade in digital data", No 2017-01, *JRC Working Papers on Digital Economy*, Joint Research Centre (Seville site).

[88] Le coût social est égal au coût total de production du bien et du service auquel s'ajoute le coût des externalités liées à la production.

[89] Omri Ben-Shahar, 2019, "Data Pollution", *Journal of Legal Analysis*, Volume 11, 104-59.

[90] Par exemple, lorsqu'ils autorisent les sites Web à collecter des informations sur leurs réseaux sociaux.

[91] Cour de justice de l'Union européenne, MetaPlatforms Inc.e.a, contre Bundeskartellamt, Arrêt C252/21, 4 juillet 2023.

1. DES OBJECTIFS QUI CONVERGENT

127. En premier lieu, le libre jeu de la concurrence, quand il peut être assuré, favorise, dans certaines conditions, la protection des données personnelles[92].

128. En effet, dans la mesure où les utilisateurs privilégient – toutes choses égales par ailleurs – les services qui respectent le plus leur vie privée, certaines entreprises peuvent chercher à se différencier en affichant une meilleure protection de la vie privée que leurs concurrents, par exemple en limitant la collecte et le traitement de données personnelles. D'autres entreprises peuvent également concevoir des innovations technologiques qui promeuvent une meilleure protection des données (par exemple, des technologies de chiffrement de bout en bout). La pression concurrentielle entre acteurs est alors de nature à susciter de telles innovations[93].

129. En second lieu, en ce qu'elle veille à l'exercice et au maintien d'une concurrence saine et loyale, la politique de la concurrence permet d'œuvrer à la protection de la vie privée dans le cadre de l'examen d'opérations de concentration ou de pratiques anticoncurrentielles.

130. Dans le cas du contrôle des concentrations, le pouvoir de marché peut notamment être apprécié sous le prisme de la collecte et de la protection des données personnelles. En particulier, une autorité de concurrence peut être amenée à évaluer la capacité d'un groupe à collecter et traiter des données personnelles, notamment en tirant avantage de la fusion de ses bases de données[94]. Une opération de concentration pourrait en effet aboutir à une accumulation des données par une entreprise, qui serait matériellement impossible ou trop coûteuse à répliquer par ses concurrents sur le marché.

131. À titre illustratif, dans sa décision du 6 septembre 2018 relative à l'opération Apple/Shazam[95], la Commission a estimé que, même si à la suite de l'opération de concentration, Apple utilisait certains de ses actifs (en particulier ses données relatives aux utilisateurs) pour renforcer la position de Shazam sur le marché de la publicité en ligne pour les amateurs de musique, cela n'aurait pas d'incidence sur la compétitivité de Shazam et cela n'entraverait pas de manière significative une concurrence effective. La Commission a en effet constaté qu'un certain nombre de grandes entreprises offrant des services de publicité en ligne sur des inventaires bien plus importants que Shazam, y compris Google et Facebook,

---

[92] Avec la limite énoncée plus haut que le marché peut converger vers un équilibre qui ne correspond pas nécessairement à un niveau élevé de protection de la vie privée.

[93] La section II.A.2 relève cependant le contexte particulier dans lequel s'exerce la pression concurrentielle sur ce paramètre. En particulier, la présence d'externalités est une défaillance qui peut faire obstacle au fait que le marché, par le libre jeu de la concurrence, aboutisse au niveau optimal de protection des données et de la vie privée (sous ou sur protection de la vie privée selon la nature des externalités), ce qui justifie la régulation.

[94] Rapport conjoint du Bundeskartellamt et de l'Autorité de la concurrence du 10 mai 2016, « *Droit de la concurrence et données* ».

Sur l'importance de la collecte et du traitement des données comme élément de pouvoir de marché, voir également le rapport « *Publicité en ligne : pour un marché à armes égales* » commandé par le gouvernement français et publié en novembre 2020, lequel considère que « *la première source de pouvoir de marché des plateformes réside dans leur capacité à collecter, croiser et exploiter des données nombreuses et variées* ». Dans ce rapport, la mission propose, afin de rééquilibrer durablement le marché, « *d'encadrer fortement le croisement de données collectées par différents services des plateformes et de considérer les données comme des actifs dont l'accès devrait être ouvert, au moins en partie, à d'autres acteurs* ».

[95] Décision COMP/M.8788 – Apple/ Shazam, 6 septembre 2018, paragraphe 38.

permettaient aux annonceurs de cibler des publics spécifiques en fonction de leurs intérêts et notamment les amateurs de musique.[96]

132. Dans sa décision du 17 décembre 2020[97], la Commission a en revanche conditionné l'acquisition de Fitbit par Google au respect intégral d'une série d'engagements proposés par Google, dont certains visaient à encadrer l'utilisation par Google des données relatives à la santé et au bien-être des utilisateurs récoltées à partir d'appareils de technologie portable à porter au poignet et d'autres appareils Fitbit[98].

133. L'accumulation et l'utilisation des données peuvent également être prises en compte dans l'examen de potentiels abus de position dominante, par exemple des conditions de transaction inéquitables[99] ou des prix excessifs[100].

134. À titre d'exemple, dans sa décision précitée du 7 février 2019, le Bundeskartellamt a sanctionné Facebook pour un abus de position dominante ayant consisté à combiner des

---

[96] Dans une décision antérieure relative à l'opération de concentration entre Facebook et Whatsapp (décision COMP/M.7217 – Facebook/WhatsApp, 3 octobre 2014), la Commission avait également examiné la capacité du groupe à tirer avantage de la fusion de bases de données et conclu à l'absence de problème de concurrence. Elle avait alors conclu que l'opération ne posait pas de problèmes de concurrence, dans la mesure où il demeurait notamment un grand nombre de données d'utilisateurs d'internet utiles pour la publicité qui n'étaient pas sous le contrôle exclusif de Facebook..

[97] Décision COMP/M.9660 – Google/Fitbit, 17 décembre 2020.

[98] En particulier, dans le cadre de cette décision, les engagements de Google en matière de publicité prévoient que : (1) Google n'utilise pas aux fins de Google Ads les données relatives à la santé et au bien-être des utilisateurs de l'EEE qui sont récoltées à partir d'appareils de technologie portable à porter au poignet et d'autres appareils Fitbit ; cela vaut également pour la publicité contextuelle, l'affichage publicitaire et les produits d'intermédiation publicitaire. Les données récoltées au moyen de capteurs (y compris le GPS) ainsi que les données introduites manuellement sont également concernées ; (2) Google maintient une séparation technique des données concernées d'utilisateurs de Fitbit. Les données seront stockées dans un «silo de données» qui sera isolé de toute autre donnée de Google utilisée à des fins publicitaires ; (3) Google veille à ce que les utilisateurs de l'Espace économique européen (ci-après, l'«EEE») aient effectivement le choix d'autoriser ou de refuser que ces données de santé et de bien-être stockées dans leur profil d'utilisateur Google ou Fitbit soient utilisées par d'autres services de Google (tels que Google Search, Google Maps, Google Assistant et YouTube).

S'agissant de l'accès à l'API web, Google s'est engagé à maintenir la possibilité, pour les applications logicielles, d'accéder, via l'API web Fitbit, aux données concernant la santé et la forme physique des utilisateurs, et ce, sans frais d'accès et sous réserve du consentement des utilisateurs.

[99] Le rapport conjoint du Bundeskartellamt et de l'Autorité souligne que « *les règles en matière de protection des données personnelles pourraient constituer une référence utile pour évaluer une pratique abusive, notamment dans un contexte où la plupart des consommateurs ne lisent pas les conditions générales de vente ni les politiques de confidentialité des différents prestataires de services qu'ils utilisent* » (Rapport conjoint du Bundeskartellamt et de l'Autorité de la concurrence du 10 mai 2016, « *Droit de la concurrence et données* »). Robertson, V. (2020), « Excessive Data Collection: Privacy Considerations and Abuse of Dominance in the Era of Big Data », *Common Market Law Review*, vol. 57, pp. 161–189.

[100] Cette qualification pose de nombreuses difficultés pratiques. D'une part, elle nécessite de déterminer un prix monétaire unique aux données (voir par exemple OECD, 'Exploring the Economics of Personal Data : A Survey of Methodologies for Measuring Monetary Value' OECD Digital Economy Papers No 220, 2 April 2013) malgré l'hétérogénéité des préférences en matière de protection des données personnelles. D'autre part, elle nécessite de trouver un marché comparable, ou de pouvoir opérer des comparaisons complexes entre prix et coûts ainsi que de définir des prix « de référence » (Rapport conjoint du Bundeskartellamt et de l'Autorité de la concurrence du 10 mai 2016, « *Droit de la concurrence et données* » ; Robertson, V. (2020), « Excessive Data Collection: Privacy Considerations and Abuse of Dominance in the Era of Big Data », *Common Market Law Review*, vol. 57, pp. 161–189.).

données personnelles d'utilisateurs provenant de différentes sources sans leur consentement[101].

2. DES TENSIONS POTENTIELLES ENTRE PROTECTION DE LA VIE PRIVEE ET CONCURRENCE

135. Dans certaines conditions, la poursuite d'un objectif de protection de la vie privée pourrait être utilisée par certaines entreprises pour commettre des pratiques anticoncurrentielles (a). En outre, la mise en œuvre d'une régulation relative à la protection des données personnelles et/ou de la vie privée peut avoir un impact sur les dynamiques concurrentielles que la politique de concurrence cherche à préserver (b).

a) La mise en œuvre de pratiques anticoncurrentielles sous couvert d'un objectif de protection de la vie privée

136. L'Autorité a déjà pu indiquer que, dans certaines conditions, des pratiques mises en œuvre sous couvert d'un objectif de protection de la vie privée pouvaient avoir des effets anticoncurrentiels.

137. À titre d'exemple, l'Autorité a été saisie le 23 octobre 2020, au fond et en mesures conservatoires, par plusieurs associations contestant la sollicitation ATT (pour « *App Tracking Transparency* ») mise en œuvre par Apple[102] aux applications sur iOS souhaitant suivre l'activité de l'utilisateur sur des sites tiers. Dans le cadre de cette saisine, ces associations soutiennent notamment que ce dispositif constitue un abus de position dominante, en ce qu'elle impose des conditions de transaction inéquitables au sens du paragraphe a) de l'article 102 du Traité sur le fonctionnement de l'Union européenne (ci-après, « TFUE ») dans la mesure où cette sollicitation n'est ni nécessaire, ni proportionnée pour atteindre l'objectif de protection de la vie privée des utilisateurs poursuivi par Apple.

138. Dans sa décision de mesures conservatoires, prise après avis de la CNIL, l'Autorité a notamment reconnu que la protection de la vie privée des utilisateurs pouvait constituer un objectif légitime poursuivi par les entreprises[103]. Elle a, en l'état des éléments du dossier, rejeté la demande de mesures conservatoires mais décidé de poursuivre l'instruction au fond du dossier[104].

---

[101] Bundeskartellamt, 6 fév. 2019, déc. n° B6-22/16.

[102] Communiqué de presse de l'Autorité du 17 mars 2021.

https://www.autoritedelaconcurrence.fr/fr/communiques-de-presse/ciblage-publicitairemise-en-place-par-apple-de-la-sollicitation-att-lautorite.

[103] Décision n° 21-D-07 précitée, paragraphe 156.

[104] Communiqué de presse de l'Autorité du 17 mars 2021, https://www.autoritedelaconcurrence.fr/fr/communiques-de-presse/ciblage-publicitairemise-en-place-par-apple-de-la-sollicitation-att-lautorite.

b) Un renforcement de la protection des données personnelles et de la vie privée peut affecter le fonctionnement concurrentiel des marchés

139. Les effets de l'entrée en vigueur du RGPD sur la concurrence sont relativement connus. Une étude, publiée en 2020[105], identifie ainsi plusieurs dynamiques de marché parallèles et cumulatives susceptibles de limiter la concurrence et d'accroître la concentration du marché à la suite du renforcement des politiques de protection des données personnelles.

140. En premier lieu, de telles politiques peuvent induire des coûts élevés de mise en conformité des entreprises, plus facilement amortis par les acteurs les plus importants du marché du fait d'économies d'échelle, mais dissuasifs pour les nouveaux entrants. La dissymétrie entre acteurs est renforcée par les incertitudes liées à la mise en place d'une protection règlementaire complexe, auxquelles les grosses entreprises peuvent plus facilement faire face. Elles peuvent utiliser ces incertitudes de manière stratégique, en limitant le partage de leurs données sur la base d'interprétations extensives du RGPD.

141. En deuxième lieu, en rendant plus difficile voire illégale l'utilisation de certaines méthodes de collecte de données, des politiques de protection telles celle mise en place par le RGPD peuvent créer des avantages comparatifs pour certains acteurs en favorisant certains modèles d'affaires. À cet égard, dans son avis de 2018 portant sur l'exploitation des données dans le secteur de la publicité sur internet, l'Autorité a indiqué que « [s]*i les problématiques de protection de la vie privée ne relèvent pas, par elles-mêmes de la compétence de l'Autorité, elle souhaite mettre en garde sur les effets que peuvent avoir les modalités de limitation ou d'encadrement de la collecte de données : en effet, selon le moyen sélectionné, certaines entreprises pourraient être désavantagées par rapport à d'autres, ce qui pourrait modifier durablement la dynamique concurrentielle* »[106]. Sur ce point, l'Autorité a également ajouté que « [s]*i l'établissement de règles permettant d'obtenir le consentement éclairé de l'internaute vis-à-vis de la collecte de données le concernant doit être soutenu comme une avancée pour la protection de la vie privée, il est également important d'instaurer des règles ne favorisant pas de manière excessive ou indue certains acteurs par rapport à d'autres* »[107].

142. En troisième lieu, les politiques de protection peuvent aussi réduire les incitations des entreprises à partager les données collectées. En effet, d'une part, les acteurs qui partagent des données sont toujours tenus de surveiller leur utilisation par toute personne avec laquelle les données sont partagées. D'autre part, même lorsque les données sont partagées, il peut être coûteux ou compliqué d'obtenir le consentement éclairé des personnes concernées au partage de leurs données, ce qui conduit à en limiter l'utilisation. Ceci peut être bénéfique pour les consommateurs, dont les données et la vie privée sont ainsi protégées mais peut aussi nuire à l'émergence de certains produits innovants reposant sur l'utilisation de telles données.

143. Enfin, à la suite de la mise en œuvre du RGPD, les personnes sont rendues plus attentives à la collecte de leurs données personnelles. Ceci pourrait en particulier les conduire à n'accepter de fournir leurs données qu'à des organisations ou à des entreprises avec lesquelles elles ont l'habitude d'interagir déjà bien implantées et qui jouissent d'une certaine réputation (généralement les plus grosses ou plus connues), au détriment notamment des nouveaux entrants.

---

[105] Gal, Michal and Aviv, Oshrit, "The Competitive Effects of the GDPR" (March 4, 2020*). Journal of Competition Law and Economics* (2020), pages de 2 à 6.

[106] Avis n° 18-A-03 précité, paragraphe 280.

[107] Avis n° 18-A-03 précité, paragraphe 293.

144. Ces constats ne visent évidemment pas à remettre en cause l'existence et la finalité du RGPD, qui, comme indiqué au paragraphe 86, reflète une mise en balance de plusieurs intérêts légitimes.

145. Toutefois, l'Autorité appelle à une vigilance concernant les effets concurrentiels de mesures allant au-delà de ce qui est strictement imposé par le RGPD, notamment lorsqu'elles seraient mises en œuvre de manière privée par des acteurs prépondérants.

146. En particulier, il convient de s'assurer de ce que les politiques de protection de la vie privée ne conduisent pas à des distorsions de concurrence nuisibles, *in fine*, aux consommateurs (en particulier dans des marchés où la concurrence est déjà amoindrie par les effets caractérisant certains marchés numériques décrits en section II.A.2). La politique de concurrence a, à cet égard, un rôle légitime à jouer.

3. UNE COORDINATION ENTRE LES DEUX CHAMPS REGLEMENTAIRES DESORMAIS ENCADREE PAR LA JURISPRUDENCE : L'ARRET META

147. Les juridictions nationales et européennes ont également été amenées, dans le contexte exposé ci-dessus, à s'interroger sur la coordination entre les autorités de contrôle nationales en matière de protection des données et les autorités de concurrence.

148. À cet égard, l'arrêt Meta est particulièrement important.

149. Le Bundeskartellamt avait engagé une procédure contre Meta, à l'issue de laquelle, par une décision du 6 février 2019, il lui a interdit, en particulier, de subordonner, dans ses conditions générales, l'utilisation du réseau social Facebook par des utilisateurs privés résidant en Allemagne au traitement de leurs données « *off Facebook*[108] » et de procéder, sans leur consentement, au traitement de ces données. Le Bundeskartellamt a également imposé à Meta d'adapter ces conditions générales afin qu'il en ressorte clairement que lesdites données ne seraient ni collectées, ni mises en relation avec les comptes d'utilisateurs Facebook, ni utilisées sans le consentement de l'utilisateur concerné.[109]

150. Le Bundeskartellamt a considéré que le traitement par Meta des données « *off Facebook* » des utilisateurs concernés, matérialisé dans ses conditions générales, constituait une exploitation abusive de sa position dominante sur le marché des réseaux sociaux en ligne pour les utilisateurs privés en Allemagne, ne pouvant pas être justifié au regard du RGPD.[110]

151. Saisi d'un recours contre la décision du Bundeskartellamt, le tribunal régional supérieur de Düsseldorf a saisi la CJUE d'une question préjudicielle, relative à la compétence d'une autorité nationale de concurrence pour constater une violation du RGPD dans le cadre du contrôle des abus de position dominante ainsi que pour ordonner la cessation de l'infraction, alors qu'elle n'est pas une autorité de contrôle au sens de l'article 51 du RGPD.

---

[108] Meta Platforms Ireland gère l'offre Facebook dans l'Union européenne. En s'y inscrivant, les utilisateurs acceptent les conditions générales et, par conséquent, les politiques d'utilisation des données et des cookies. En vertu de celles-ci, Meta Platforms Ireland collecte des données relatives aux activités des utilisateurs à l'intérieur, et à l'extérieur du réseau social (« *off Facebook* »), et les met en relation avec les comptes Facebook des utilisateurs concernés.

[109] Arrêt Meta (C-252/21) précité, paragraphe 29.

[110] Arrêt Meta (C-252/21) précité, paragraphe 30.

152. Dans son arrêt Meta, la CJUE a jugé qu'une autorité nationale de concurrence peut constater, dans le cadre de l'examen d'un abus de position dominante, une violation du RGPD, lorsque ce constat est important pour établir l'existence d'un tel abus[111]. À cet égard, la Cour indique notamment « [qu']*une autorité de la concurrence doit apprécier, sur la base de toutes les circonstances spécifiques de l'affaire, si le comportement de l'entreprise en position dominante a pour effet de faire obstacle, par le recours à des moyens différents de ceux qui gouvernent une compétition normale des produits ou des services, au maintien du degré de concurrence existant sur le marché ou au développement de cette concurrence* (…). *À cet égard, la conformité ou la non-conformité d'un tel comportement aux dispositions du RGPD peut constituer, le cas échéant, un indice important parmi les circonstances pertinentes de l'espèce pour établir si ce comportement constitue un recours à des moyens qui gouvernent une compétition normale ainsi que pour évaluer les conséquences d'une certaine pratique sur le marché ou pour les consommateurs* »[112].

153. La CJUE précise également que « *l'accès aux données à caractère personnel et la possibilité de traitement de ces données sont devenus un paramètre significatif de la concurrence entre entreprises de l'économie numérique. Partant, exclure les règles en matière de protection des données à caractère personnel du cadre juridique à prendre en considération par les autorités de la concurrence lors de l'examen d'un abus de position dominante méconnaîtrait la réalité de cette évolution économique et serait susceptible de porter atteinte à l'effectivité du droit de la concurrence au sein de l'Union* ».[113]

154. La CJUE ajoute néanmoins que, si dans le cadre de l'examen d'un abus de position dominante de la part d'une entreprise sur un marché déterminé, l'autorité de la concurrence de l'État membre peut avoir à examiner également la conformité aux règles de protection des données à caractère personnel prévues par le RGPD[114], elle ne se substitue pas aux autorités de contrôle mises en place par ce règlement lorsqu'elle relève une violation du RGPD. En effet, son appréciation doit se limiter aux seules fins de constat d'un abus de position dominante et d'imposition de mesures correctrices selon les règles du droit de la concurrence.

155. En outre, la CJUE décrit les modalités pratiques d'une coopération entre les autorités nationales de concurrence et de contrôle en matière de protection des données.

156. Notamment, l'autorité nationale de concurrence :

- est tenue par le principe de coopération loyale avec l'autorité de contrôle concernée, afin d'assurer une application cohérente du RGPD[115] ;
- doit prendre en considération toute décision ou enquête de l'autorité de contrôle compétente en vertu du RGPD. Notamment, dans l'hypothèse où une autorité de la concurrence nationale considère nécessaire de se prononcer, dans le cadre d'une décision relative à un abus de position dominante, sur la conformité ou la non-conformité au RGPD d'un traitement de données à caractère personnel effectué par une entreprise, elle doit vérifier si ce comportement ou un comportement

[111] Arrêt Meta (C-252/21) précité, paragraphe 62.

[112] Arrêt Meta (C-252/21) précité, paragraphe 47, soulignement ajouté.

[113] Arrêt Meta (C-252/21) précité, paragraphe 51.

[114] Arrêt Meta (C-252/21) précité, paragraphe 48.

[115] Arrêt Meta (C-252/21) précité, paragraphe 52.

similaire a déjà fait l'objet d'une décision par l'autorité de contrôle compétente ou bien encore par la Cour. Si tel est le cas, elle ne peut s'en écarter, tout en restant libre d'en tirer ses propres conclusions sous l'angle de l'application du droit de la concurrence[116].

C. ANALYSE DES RECOMMANDATIONS PROPOSEES PAR LA CNIL

157. L'Autorité considère que le projet de la CNIL doit être salué, notamment en ce qu'il clarifie les responsabilités et obligations des acteurs du secteur au sens du RGPD et de l'article 82 de la Loi Informatiques et Libertés, dans le contexte particulier des applications mobiles[117], en fournissant un grand nombre d'exemples concrets. Ce projet répond par ailleurs à un besoin exprimé par ces acteurs. En ce sens, le projet vise dans son ensemble à favoriser une meilleure protection des données personnelles de l'utilisateur.

158. À titre liminaire, l'Autorité rappelle que lorsqu'elle est consultée pour avis, comme en l'espèce, elle ne peut se prononcer que sur des questions de concurrence d'ordre général. Il ne lui appartient pas, dans ce cadre, de statuer sur le point de savoir si telle ou telle pratique est ou serait contraire au droit de la concurrence. Seules une saisine contentieuse et la mise en œuvre de la procédure prévue par les articles L. 463-1 et suivants du code de commerce sont, en effet, de nature à permettre une telle appréciation.

159. Par conséquent, cet avis ne se prononce pas sur des comportements particuliers ou sur des pratiques potentiellement anticoncurrentielles spécifiques, mais se limite à préciser les risques présentés par certaines recommandations pour le fonctionnement concurrentiel des marchés concernés. Enfin, quand bien même cet avis identifie de potentielles préoccupations, l'Autorité rappelle que toute évaluation d'une pratique au regard du droit de la concurrence ne peut se faire qu'en tenant compte des caractéristiques particulières du ou des marchés concernés afin d'en évaluer, au cas par cas, l'existence d'une éventuelle position dominante et les effets anticoncurrentiels potentiels et/ou avérés de la pratique en question.

160. L'Autorité entend toutefois formuler, dans un premier temps, des observations préalables sur les problématiques concurrentielles générales susceptibles d'être soulevées par ce projet (1). Ces observations pourraient ainsi orienter la rédaction du texte. Par la suite, elle abordera spécifiquement certaines préoccupations concurrentielles plus particulières, concernant, notamment, les sections concernant les éditeurs (2), les fournisseurs d'OS (3), les fournisseurs de SDK (4), et les fournisseurs de magasins d'applications (5).

161. Cette analyse ne se veut pas exhaustive. Le fait qu'une ou plusieurs dispositions du projet ne fassent pas l'objet d'une analyse spécifique (comme, notamment, celles relatives à l'articulation entre permission et consentement) n'exclut pas que leur mise en œuvre puisse comporter des risques concurrentiels.

162. Enfin, dans le présent avis, l'Autorité ne s'exprime pas sur les dispositions du projet concernant les obligations issues du RGPD et de la loi Informatique et Libertés et limite son analyse aux seules dispositions constituant des « bonnes pratiques » qui devraient être mises en œuvre selon la CNIL.

---

[116] Arrêt Meta (C-252/21) précité, paragraphe 56.

[117] L'univers web a déjà fait l'objet de lignes directrices et d'une recommandation de la CNIL en matière de « cookies et autres traceurs ».

1. REMARQUES PREALABLES SUR LES PROBLEMATIQUES CONCURRENTIELLES SUSCEPTIBLES D'ETRE SOULEVEES PAR LE PROJET

163. L'Autorité a identifié plusieurs sujets généraux se référant directement ou indirectement aux recommandations de la CNIL, qu'elle souhaite aborder brièvement ci-après. Après mention de l'application du droit de la concurrence dans le cadre du projet (a), l'Autorité souhaite appeler l'attention de la CNIL sur le rôle en matière de protection de la vie privée accordé par le projet à certains acteurs du secteur qui, compte tenu de la structure concurrentielle de ce dernier, sont susceptibles de détenir un fort pouvoir de marché (b). En outre, l'Autorité appelle la CNIL à une vigilance sur l'application du DMA (c), sur l'impact de son projet sur les acteurs basés en France (d), et sur la différence de cadre réglementaire auquel ce projet pourrait conduire selon les environnements (e).

a) Sur la référence au respect du droit de la concurrence dans le projet

164. S'agissant de la prise en compte de l'application du droit de la concurrence dans le cadre de son projet, la CNIL indique en introduction des sections 8 et 9 :

« *Ces recommandations s'appliquent sans préjudice des règles applicables sur d'autres fondements juridiques que la protection des données personnelles, notamment le droit de la concurrence* ».

L'Autorité salue cette mention mais considère qu'elle devrait viser l'ensemble des recommandations de la CNIL.

b) Sur la prise en compte de la structure concurrentielle du secteur des applications mobiles et sur le rôle accordé par le projet à certains acteurs de ce secteur en matière de protection de la vie privée

165. En premier lieu, comme indiqué à la section I.A, les fournisseurs de magasins d'applications mobiles et/ou d'OS jouent, dans le secteur des applications mobiles, un rôle d'intermédiaires entre les éditeurs d'applications et les utilisateurs. En outre, les principaux fournisseurs de magasins d'applications mobiles et/ou d'OS sont des acteurs verticalement intégrés le long de la chaîne de valeur des applications mobiles et pourraient, dans certaines conditions, détenir un pouvoir de marché important (voire être considérés comme dominants) sur certains marchés de cette chaîne de valeur. Apple et Google sont ainsi à la fois fournisseurs d'OS, fournisseurs de magasins d'applications, fournisseurs de SDK, éditeurs, développeurs et fournisseurs d'autres services. Ils ont par ailleurs été désignés contrôleurs d'accès au sens du DMA pour plusieurs services de l'environnement applicatif mobile.

166. Ces opérateurs se trouvent de ce fait déjà dans une position asymétrique favorable par rapport aux autres acteurs du secteur, notamment certains développeurs et éditeurs. Ces derniers sont en effet soumis aux conditions d'accès imposées par ces plateformes.

167. En second lieu, le projet accorde aux fournisseurs d'OS et aux magasins d'applications un rôle important en matière de protection de la vie privée qui ne découle pas directement d'obligations conférées par la réglementation en vigueur relative à la protection des données personnelles, et notamment par le RGPD.

168. Toutefois, quand bien même les interactions entre éditeurs d'applications et intermédiaires (fournisseurs d'OS et/ou de magasins d'applications mobiles) peuvent conduire ces derniers

à jouer un rôle dans la mise en œuvre du RGPD par les éditeurs (sur qui pèsent les obligations du RGPD), ce rôle ne doit pas aboutir à distordre la concurrence sur les marchés en cause ou à leur conférer un pouvoir de marché supplémentaire. À cet égard, les recommandations concernant des mesures de protection de la vie privée qui vont au-delà des obligations règlementaires devraient se garder de toute mesure qui viendrait accroître le pouvoir de marché des opérateurs.

169. Or, comme il ressort des échanges avec les acteurs, le projet est susceptible, dans certaines conditions, de conférer un pouvoir discrétionnaire et prescriptif important à certains opérateurs.

170. En ce sens, et sans que cela résulte d'obligations réglementaires, le projet pourrait conduire à renforcer les asymétries entre les acteurs du secteur, au détriment des acteurs non intégrés verticalement.

171. Par ailleurs, dans la mesure où certaines recommandations conduisent à la mise en œuvre d'obligations supplémentaires à ce qu'exige la réglementation applicable, elles soulèvent la question des effets de cet incrément d'obligations sur les barrières à l'entrée ou à l'expansion.

172. En outre, de nombreux acteurs entendus ont souligné que les dispositions de la CNIL pourraient être utilisées par ces opérateurs verticalement intégrés à des fins anticoncurrentielles, notamment pour s'accorder un avantage et/ou imposer des contraintes à leurs partenaires plus restrictives que celles qu'ils s'appliquent à eux-mêmes. Certains opérateurs ont également indiqué qu'il faudrait s'assurer que la mise en œuvre du projet n'amène pas les acteurs verticalement intégrés à imposer leurs normes ou leurs solutions.

173. Sur ces éléments, l'Autorité rappelle, comme elle a déjà pu l'indiquer par le passé, qu'un opérateur, y compris en position dominante, est libre d'édicter les règles qu'il estime utiles pour conditionner l'accès à ses biens ou ses services, sous réserve que leur mise en œuvre n'ait pas pour objet ou pour effet de restreindre la concurrence. Cette liberté n'exonère toutefois pas ces opérateurs de l'obligation de mettre en œuvre leurs règles dans des conditions objectives, transparentes et non discriminatoires[118].

174. Dans ce cadre, l'Autorité souligne la responsabilité particulière qui pèse sur les acteurs dominants, lesquels doivent veiller à ne pas porter atteinte, par leur comportement, à une concurrence effective et non faussée. En particulier, lorsque ces acteurs décident d'imposer des restrictions à l'utilisation de leurs services ou plateformes, susceptibles d'affecter le fonctionnement concurrentiel normal du marché, celles-ci doivent être objectives, proportionnées, transparentes et non discriminatoires. Par ailleurs, l'Autorité rappelle également les obligations particulières résultant des dispositions du DMA qui incombent aux acteurs désignés contrôleurs d'accès.

[118] Voir les décisions n° 21-D-07 précitée, paragraphes 134 à 138 et n° 19-D-26 du 19 décembre 2019 relative à des pratiques mises en œuvre dans le secteur de la publicité en ligne liée aux recherches, paragraphes 334 à 336.

En conclusion, l'Autorité considère que le projet devrait, dans son approche, davantage tenir compte de la structure concurrentielle du secteur, et en particulier de la position de certains acteurs.

Dans ce contexte, l'Autorité invite la CNIL à ce que ses recommandations ne confèrent pas un pouvoir supplémentaire à des acteurs disposant déjà d'un fort pouvoir de marché, notamment à ceux pouvant être considérés comme étant en position dominante, et qui pourraient être susceptibles de s'appuyer sur cette recommandation à des fins anticoncurrentielles.

L'Autorité considère également souhaitable que la CNIL mentionne expressément que ses recommandations s'appliquent de la même manière aux applications mobiles propriétaires des fournisseurs d'OS ou de magasins d'applications qu'aux applications tierces, afin d'éviter que celles-ci soient utilisées par certains opérateurs pour mettre en œuvre un traitement différencié susceptible d'avantager les applications mobiles propriétaires (*self-preferencing*).

c) Sur l'application du DMA

175. Certains acteurs entendus ont indiqué que le projet de la CNIL prendrait pour acquis un état de fait résultant du pouvoir qu'auraient Google et Apple en tant que « contrôleurs d'accès » alors que la situation concurrentielle dans laquelle ces deux acteurs opèrent est dégradée et a contribué à motiver la création du DMA. La CNIL entérinerait donc l'acquisition du pouvoir de marché de ces acteurs, que le règlement vise à encadrer, voire réduire.

176. De plus, certains acteurs considèrent qu'en application de ses recommandations, la CNIL délèguerait des pouvoirs de régulation à ces contrôleurs d'accès. Elle accroîtrait ainsi l'asymétrie entre les acteurs à leur profit, à l'inverse des objectifs du DMA.

177. Enfin, certains acteurs considèrent que certaines dispositions seraient contraires à des articles du DMA, notamment aux articles 5(2)(b), 6(2) et 6(12).

178. L'Autorité constate également certaines contradictions entre le projet de la CNIL et le DMA, non seulement s'agissant du pouvoir conféré aux contrôleurs d'accès, mais également avec certaines dispositions spécifiques (des exemples concrets sont fournis dans les développements qui suivent).

Sur ces éléments, l'Autorité invite la CNIL à prêter une attention particulière à ce que ses recommandations n'aient pas l'effet de déléguer sa compétence, en tant que régulateur national, aux contrôleurs d'accès, au risque de renforcer les asymétries de pouvoir de marché au bénéfice de ces derniers.

d) Sur la mise en œuvre de la recommandation de la CNIL par les acteurs ayant leur siège hors UE et le potentiel impact de sa recommandation pour les acteurs basés en France

179. Selon certains acteurs interrogés, la CNIL a établi une recommandation sur la base de sa propre interprétation du RGPD alors qu'aucune autre autorité de contrôle en matière de protection des données dans l'Union européenne n'aurait établi un document équivalent.

180. En outre, un certain nombre d'acteurs ont relevé que leurs concurrents, ayant leur siège à l'étranger mais fournissant leurs services en France, ne seraient pas soumis au respect de la

recommandation de la CNIL puisque, en application du principe du guichet unique prévu par le RGPD, la CNIL ne pourrait contrôler que les entités ayant un siège en France. Il ressort ainsi des échanges menés par l'Autorité que la recommandation de la CNIL serait susceptible de créer des contraintes supplémentaires pour les acteurs français, pesant sur leur compétitivité. Il pourrait en résulter un risque de retrait du marché français pour certains acteurs, pour lesquels le marché français ne représenterait pas une part importante de leur chiffre d'affaires ainsi qu'une barrière à l'entrée supplémentaire pour offrir ses services sur le marché français.

181. Par ailleurs, les acteurs basés hors de France pourraient avoir une certaine latitude pour ne mettre en œuvre que les dispositions susceptibles d'avoir un intérêt pour eux, ce qui limiterait la portée de la recommandation de la CNIL.

Sur ces éléments, l'Autorité accorde une importance particulière au fait que ses recommandations ne viennent pas créer des barrières à l'entrée supplémentaires pour de nouveaux entrants sur le marché français ni de désavantage en termes de coûts ou de contraintes pour les entreprises établies en France.

e) Sur la différence de cadre réglementaire entre l'environnement Web (*via* navigateur) et l'environnement applicatif mobile

182. Il ressort des échanges avec les acteurs qu'une grande partie d'entre eux s'interrogent sur les raisons conduisant la CNIL à avoir une approche différente, dans ses recommandations[119], entre l'environnement Web (*via* navigateur) et l'environnement applicatif mobile. Dans ce cadre, certains relèvent que, contrairement à l'environnement Web (*via* navigateur), la CNIL semblerait déléguer une partie de son rôle de contrôle aux opérateurs verticalement intégrés.

183. Compte tenu de cette différence d'approche dans les différentes recommandations de la CNIL, se poserait par exemple la question du traitement des « nouveaux » OS de nature « hybride » (par exemple, selon un acteur entendu, pour Apple, Watch OS et Ipad OS). En outre, l'adoption d'une approche différente dans les recommandations concernant l'environnement applicatif mobile serait susceptible de créer des distorsions de concurrence assez importantes, en conduisant à un traitement différent selon le modèle d'affaires ou le mode de distribution.

184. Enfin, l'un des acteurs entendus a souligné que l'environnement applicatif mobile devient de plus en plus complexe par rapport à l'environnement Web (*via* navigateur), en particulier s'agissant des problématiques liées aux données. Cette considération est susceptible de conduire des acteurs à changer de stratégie et à se tourner vers d'autres environnements.

185. La différence d'approche des problématiques liées aux données entre les environnements web et applicatif mobile n'est pas un problème en soi, ainsi il n'est pas forcément nécessaire de rechercher à tout prix la neutralité technologique. Toutefois, l'Autorité estime qu'il ne faudrait pas que la complexité de la règlementation concernant les applications mobiles (et leur écosystème) crée des distorsions de concurrence entre les environnements qui pourraient conduire certains éditeurs à modifier leur comportement au détriment des consommateurs, par exemple avec pour objectif de contourner les règles appliquées aux applications mobiles.

[119] Comme déjà indiqué supra, l'univers web a par exemple déjà fait l'objet de lignes directrices et d'une recommandation de la CNIL en matière de « cookies » et autres traceurs.

Ceci pourrait conduire des acteurs à éviter l'écosystème mobile et réduire ainsi la diversité de l'offre proposée aux utilisateurs.

Pour ces raisons, l'Autorité invite la CNIL à s'assurer que ces recommandations ne risquent pas (i) de créer des distorsions de concurrence entre les univers mobile et web et/ou (ii) d'engendrer des barrières supplémentaires à l'entrée ou à l'expansion dans l'environnement applicatif mobile.

2. SUR LA SECTION CONCERNANT LES EDITEURS

186. Les éditeurs sont les premiers responsables du recueil du consentement de l'utilisateur.

187. Dans ce contexte, les éditeurs entendus considèrent que l'application des recommandations de la CNIL serait susceptible de renforcer le rôle d'intermédiaire du fournisseur d'OS entre éditeur et utilisateur, en réduisant ainsi leur lien direct avec les utilisateurs. Les recommandations de la CNIL devraient en conséquence veiller à ce que le lien entre les éditeurs et les utilisateurs de leurs applications ne soit pas dégradé par leur mise en œuvre.

188. S'agissant des recommandations concernant spécifiquement les éditeurs, l'attention de l'Autorité et des acteurs entendus a été particulièrement appelée sur la section 5.1.3 « *Appliquer les principes de protection des données dès la conception et par défaut* », où la CNIL indique 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* ».

189. Ce point inquiète notamment les éditeurs de jeux cross plateformes qui craignent que cette disposition leur impose de renoncer à un identifiant utilisateur ayant pour conséquence une forte dégradation de l'expérience de jeu pour l'utilisateur.

190. L'Autorité reconnaît les mérites ainsi que les désavantages des environnements logués d'un point de vue concurrentiel[120]. À titre d'exemple, dans son avis sur l'exploitation des données dans le secteur de la publicité sur internet de 2018, l'Autorité a indiqué qu'un utilisateur logué aurait une compréhension plus immédiate du service qui lui est rendu, ce qui l'amènerait à accepter plus facilement le traitement de ses données personnelles, sans distinguer le fait que cette collecte se fasse aux fins de fourniture du service ou aux fins de traçage publicitaire, alors qu'un utilisateur non logué ne percevrait pas nécessairement que le traçage publicitaire contribue à la fourniture de revenus à l'éditeur du site qu'il visite. Cette différence de perception se traduirait par un biais favorable aux environnements logués, lorsque le consentement est recueilli[121].

191. Dans cet avis, l'Autorité a souligné également que le recueil obligatoire d'un consentement explicite de l'internaute, au niveau du navigateur, était susceptible de désavantager des acteurs fonctionnant *via* des cookies par rapport à d'autres acteurs ayant mis en œuvre des environnements logués, et ayant obtenu de l'internaute lors de son inscription un

[120] Voir pour plus des développements sur ce point l'avis n° 18-A-03 précité, paragraphes 277 à 296, pages 108 à 113.

[121] Avis n° 18-A-03 précité, paragraphe 287.

consentement perçu comme général à la collecte de ses données en contrepartie du service rendu[122].

Sur la base de ces éléments, l'Autorité considère que les éditeurs devraient avoir la possibilité de proposer un environnement logué lorsque ceci est nécessaire pour offrir un service de qualité à l'utilisateur. L'Autorité invite donc la CNIL à préciser les circonstances dans lesquelles la création de compte ne serait pas justifiée afin d'éviter des risques de restriction pour les applications dont le/les services seraient significativement dégradés sans environnement logué.

3. SUR LA SECTION CONCERNANT LES FOURNISSEURS D'OS

192. Dans son projet sur les applications mobiles, la CNIL confère aux fournisseurs d'OS un rôle important en matière de protection de la vie privée.

193. À titre liminaire et comme déjà indiqué dans les observations préliminaires (section II.C.1.b), l'Autorité souligne que ce rôle ne résulte généralement pas d'obligations conférées par la réglementation applicable en la matière, et en particulier par le RGPD et la loi Informatique et Libertés.

194. En effet, comme le précise la CNIL dans son projet à la section 8.3, « *dans de nombreux cas, le fournisseur d'OS n'est pas partie prenante des traitements de données personnelles opérés au sein des applications* ». Toutefois, la CNIL considère, ainsi qu'elle l'indique à la section 4.2. de ses recommandations, « [qu']*en tout état de cause, et même lorsqu'ils se limitent à fournir des outils techniques sans procéder à des traitements eux-mêmes, les fournisseurs d'OS conditionnent dans une certaine mesure, de par leurs choix techniques, la manière dont les traitements de données personnelles sont mis en œuvre par les éditeurs d'applications. Les fournisseurs d'OS sont, à ce titre, visés par certaines recommandations (voir la partie 8 des présentes recommandations : « Recommandations spécifiques au fournisseur d'OS »), indépendamment de leur responsabilité au sens du RGPD, s'agissant des configurations qu'ils déterminent (recueil des différentes permissions, accès aux API, etc.). Ces recommandations applicables aux OS sont susceptibles de constituer des obligations légales en cas de qualification de l'éditeur de l'OS de responsable du traitement* ».

195. À ce titre, la CNIL recommande aux fournisseurs d'OS d'assurer la bonne information de leurs partenaires, en particulier en fournissant de la documentation et des conseils pour la bonne utilisation des fonctionnalités proposées (section 8.2), et de mettre à disposition des outils pour permettre le respect des droits et du consentement des utilisateurs (section 8.3).

196. L'Autorité prend note de la volonté de la CNIL d'améliorer la protection de la vie privée par la mise en œuvre de bonnes pratiques sur l'ensemble de la chaîne de valeur des écosystèmes mobiles, y compris à la maille des fournisseurs d'OS.

---

[122] Avis n° 18-A-03 précité, paragraphe 294. L'Autorité estimait en outre que « *l'obtention du consentement prévu par le projet de règlement devrait à tout le moins se faire site par site avec des modalités qui permettent d'assurer aux différents types d'acteurs de partir sur un pied d'égalité. Cette obligation devrait couvrir l'ensemble des traceurs et inclure les environnements logués. À défaut, d'une part les intermédiaires techniques déjà fragiles pourraient disparaître au profit des leaders qui reposent sur des environnements logués, et d'autre part les éditeurs seraient eux-mêmes probablement conduits à se tourner vers une généralisation des environnements logués, ce qui irait paradoxalement à l'encontre du souhait d'anonymat recherché par les internautes* » (page 113).

197. Cependant, l'Autorité souhaite appeler l'attention de la CNIL sur le contexte concurrentiel particulier de ce secteur, résultant de ce que les deux principaux systèmes d'exploitation, iOS et Android, sont fournis par deux grands acteurs verticalement intégrés au sein de la chaîne de valeur des applications mobiles, Apple et Google. Dans le cadre de la mise en œuvre du DMA, ces deux acteurs ont récemment été désignés contrôleurs d'accès par la Commission et ce notamment pour leurs systèmes d'exploitation iOS et Android. Ceci leur confère donc certaines obligations au regard du DMA. Ils sont, par ailleurs, susceptibles de détenir une position dominante sur un ou plusieurs marchés de la chaîne de valeur des applications mobiles[123].

198. Dans ce contexte, l'Autorité considère nécessaire de veiller à ce que les recommandations de la CNIL relatives aux fournisseurs d'OS ne puissent pas être utilisées par les fournisseurs d'OS à des fins anticoncurrentielles (par exemple, pour mettre en œuvre des traitements discriminatoires) ou ne conduisent pas à élever de façon indue des barrières à l'entrée qui renforceraient les asymétries existantes sur certains marchés de la chaîne de valeur, par ailleurs déjà concentrés.

199. En effet, comme indiqué à la section I.A.2, plusieurs autorités nationales ou européenne ont déjà soulevé des préoccupations de concurrence à l'égard des fournisseurs d'OS dans le cadre de rapports dédiés à l'écosystème mobile ou de l'examen d'affaires relatives à des dossiers antitrust. Par exemple, plusieurs autorités[124] ont exprimé des préoccupations de concurrence concernant l'accès à la technologie NFC[125] ou à la fonctionnalité de géolocalisation. Ces préoccupations de concurrence appellent à une certaine vigilance concernant l'accès aux fonctionnalités du système d'exploitation.

200. L'Autorité souligne par ailleurs que les inquiétudes des acteurs relatives aux dispositions du projet spécifiques aux fournisseurs d'OS concernent particulièrement les recommandations de bonnes pratiques adressées qui vont au-delà des obligations imposées par la réglementation en vigueur (voir également la section II.C.1.b). L'Autorité expose ci-après

---

[123] Par exemple, dans sa décision Google Android du 18 juillet 2018, la Commission a conclu que Google occupe une position dominante sur les marchés des systèmes d'exploitation mobiles intelligents sous licence et des boutiques d'applications en ligne pour le système d'exploitation mobile Android.

[124] À cet égard, l'Autorité relève que la Commission a envoyé une communication des griefs à Apple, exprimant son avis préliminaire selon lequel Apple aurait abusé de sa position dominante sur le marché des portefeuilles mobiles sur iOS en réservant l'accès à la technologie NFC à Apple Pay. La décision de la Commission n'a pas encore été rendue.

Le rapport de la CMA "*Mobile ecosystems: Market study final report"* du 10 juin 2022, s'interroge notamment sur les conditions d'accès des éditeurs aux magasins d'applications de Google et d'Apple, en particulier dans le cadre de leur processus de revue des applications, et, s'agissant de la face utilisateurs des magasins d'application, à la présentation des applications, notamment l'architecture des choix retenue. Dans ce même rapport, la CMA s'est également inquiétée du fait que les arguments relatifs à la sécurité et à la vie privée des utilisateurs pourraient justifier des décisions de nature à nuire à la concurrence ou à limiter le choix des consommateurs.

Voir également les rapports "*Competition in the mobile application ecosystem*, Department of Commerce, février 2023 et « Market Study Report on Mobile OS and Mobile App Distribution », The Japan Fair Trade Commission, février 2023.

[125] La NFC est une technologie de communication sans fil à courte portée qui permet à deux appareils compatibles NFC de transférer des informations entre eux. La NFC est une technologie fondée sur des normes, c'est-à-dire qu'elle n'est pas la propriété d'une seule entreprise. La courte portée de la technologie NFC la rend idéale pour les applications sensibles à la sécurité où la proximité est importante. Les cartes de crédit et de débit sans contact et d'autres cartes à puce utilisent cette technologie.

son analyse de plusieurs dispositions, sans exclure que d'autres dispositions de cette section puissent également avoir des effets sur les dynamiques concurrentielles.

a) Sur l'information et les conseils aux partenaires

201. À la section 8.2, la CNIL considère que « *les fournisseurs d'OS, du fait de leur expertise sur les traitements qu'ils opèrent et sur les fonctionnalités qu'ils proposent, sont les plus à même de fournir de la documentation et des conseils pour la bonne utilisation des fonctionnalités proposées* ». Elle propose un ensemble de mesures pouvant être mises en œuvre à cette fin, en tant que bonnes pratiques.

202. En particulier, à la section 8.2.1 intitulée « [f]*ournir des documentations exhaustives et claires pour favoriser la conformité des partenaires* », la CNIL indique « [qu']*afin de faciliter la bonne compréhension des fonctionnalités de l'OS, il est recommandé de mettre à disposition une documentation exhaustive et claire, tant sur le plan technique que juridique* ».

203. La CNIL précise dans cette même section que :

« *S'il est courant que des documentations techniques soient mises à disposition, peuvent y être inclues également des éléments analysant le cadre législatif et normatif particulier de l'Union européenne, pour les éditeurs et développeurs qui souhaitent cibler le marché européen.*

Ces éléments juridiques ne devraient pas être séparés des éléments techniques, et une compréhension commune des impacts qu'auront les décisions de chaque type devrait être favorisée pour permettre des décisions communes de la part de ces acteurs.

Ces éléments, et en particulier les contenus juridiques, devraient être rendus disponibles dans une langue comprise par le public visé ».

204. Sur ce sujet, un des acteurs interrogés s'inquiète du rôle trop important ainsi conféré par la CNIL au fournisseur d'OS. Il considère que le fournisseur ne serait pas en mesure d'évaluer la conformité des développeurs aux lois applicables (puisqu'il n'aurait pas les informations détaillées concernant les traitements) et qu'il appartient plutôt aux développeurs, qui disposent d'une visibilité directe sur leurs traitements de données, et à leur conseil juridique le cas échéant, de déterminer la meilleure manière de se conformer au droit applicable.

205. L'Autorité relève que le pouvoir supplémentaire qui serait ainsi confié aux fournisseurs d'OS n'a pas pour corollaire une responsabilité de ces derniers en termes de conformité au regard de la réglementation applicable.

206. En particulier, l'Autorité souhaite appeler l'attention de la CNIL sur le fait que la mise en œuvre de cette recommandation, en ce qu'elle invite le fournisseur à prodiguer des conseils et à fournir une documentation juridique complète, pourrait lui permettre d'imposer sa manière de se conformer à la réglementation aux acteurs de la chaîne de valeur et, sous couvert de mieux protéger la vie privée, de mettre en place des règles diminuant la concurrence sur le marché.

Pour ces raisons, tout en s'associant à l'objectif de bonne information des acteurs de la chaîne de valeur des applications mobiles, source de transparence des marchés, l'Autorité appelle l'attention de la CNIL sur le rôle conféré au fournisseur d'OS et, à tout le moins, invite la CNIL à préciser que les documentations fournies ne doivent pas avoir valeur de conseil juridique ni viser à imposer une manière de se conformer à la réglementation européenne.

b) Sur les permissions du fournisseur d'OS en tant qu'autorisations d'accès aux capteurs, fonctionnalités ou stockage du terminal utilisateur et leur usage pour renforcer la protection de la vie privée

207. La section 8.3.1 du projet de la CNIL vise notamment à étendre le système de permissions. La CNIL considère en effet que « *le système des permissions est au cœur de la protection des utilisateurs fournie par l'OS. À ce titre, il est important, lors de la conception de celui-ci, de mettre en œuvre le maximum de mesures permettant de protéger les données personnelles de l'utilisateur* ».

208. Dans son glossaire (section 10), la CNIL définit les permissions d'accès comme « *des dispositifs mis en œuvre par les OS des terminaux mobiles pour permettre aux utilisateurs de choisir quelles fonctionnalités sont accessibles aux applications mobiles. Ces applications mobiles n'ont en effet par défaut qu'un accès limité à ces fonctionnalités, pour des raisons de sécurité et de protection de la vie privée. L'OS met dès lors à leur disposition des API leur permettant d'effectuer des requêtes afin de se voir autoriser des fonctionnalités additionnelles, sous réserve que l'utilisateur, via une interface fournie par l'OS, l'accepte* ».

209. Sur ce sujet, certains acteurs interrogés se sont montrés favorables à la mise en œuvre d'un système de permissions clair du fournisseur d'OS, en soulignant l'impact potentiellement positif en termes d'information de l'utilisateur, sous réserve d'une contextualisation des demandes de permission. Selon certains acteurs, la mise en œuvre d'un système de permissions par le fournisseur d'OS pourrait permettre d'éviter les erreurs d'accès, d'offrir un cadre unifié à disposition des développeurs, de forcer les SDK à justifier leur besoin d'accès à une fonctionnalité ou encore à améliorer la confiance envers le fournisseur d'OS.

210. Toutefois, la plupart des acteurs ont exprimé des craintes relatives à la mise en œuvre d'un système de permissions généralisé susceptible de restreindre l'accès à certaines fonctionnalités de l'OS pour les applications des éditeurs tiers (*i*) et de décourager l'acceptation des utilisateurs à la demande de permission (*ii* et *iii*). La disposition relative à la gestion des refus de permission par le fournisseur d'OS a également suscité de nombreuses réactions défavorables des acteurs entendus (*iv*).

i. Sur la faculté du fournisseur d'OS de restreindre l'accès à certaines ressources de l'OS

211. En premier lieu, l'Autorité constate que certaines dispositions de la section 8.3.1 encouragent les fournisseurs d'OS à faire un large usage des permissions afin de contrôler les accès aux ressources OS (capteurs, fonctionnalités et stockage), en vue de protéger la vie privée des utilisateurs. Cet objectif dépasse celui du seul respect de la réglementation sur la protection des données personnelles.

212. En effet, dans cette section, la CNIL indique « [qu']*en empêchant techniquement et/ou contractuellement les éditeurs d'applications d'accéder à certaines données, les permissions apportent une garantie technique forte de respect de la confidentialité des informations par les applications, et constituent une mesure positive majeure pour préserver la vie privée des personnes* »[126].

213. Dans cette même section, la CNIL indique que « [l]*e fournisseur d'OS devrait appliquer les permissions d'accès au terminal utilisateur que ce soit à ses capteurs (appareil photo, GPS, capteurs environnementaux), ses fonctionnalités (accès réseau, Bluetooth, NFC), ou son*

[126] Soulignements ajoutés.

stockage (contacts, galerie photo, stockage de masse). (…) *Il devrait prévoir le recueil d'une permission d'accès donnée par l'utilisateur du terminal indépendamment de l'obligation légale de recueillir ou non un consentement au titre de l'article 82 de la loi Informatique et Libertés pour l'opération de lecture d'informations stockées sur le terminal* »[127].

214. Sur ce point, l'Autorité relève que la mise en œuvre d'un système généralisé de permissions soulève la question de l'accès réservé aux ressources qui seraient exclues du champ du système de permissions.

215. Plus précisément, il convient de clarifier si, dans le cadre de ce système de permissions étendu, les ressources non soumises au système de permissions sont considérées par défaut comme librement accessibles ou non à l'ensemble des éditeurs. Dans ce second cas, les ressources OS existantes non incluses dans le champ des permissions seraient alors *de facto* réservées au fournisseur d'OS.

216. L'Autorité souhaite appeler l'attention sur l'importance de cette clarification, dans la mesure où le fournisseur d'OS, acteur verticalement intégré, pourrait, en se réservant la possibilité de ne pas soumettre certaines de ses ressources à ce système de permissions généralisé, mais en accordant cet accès à ses applications propriétaires, mettre en œuvre un traitement discriminatoire.

217. Sur ce sujet, certains acteurs craignent que les fournisseurs d'OS puissent utiliser le système de permissions pour refuser aux éditeurs, sous couvert d'un objectif de protection de la vie privée dès la conception ou par défaut, de leur donner accès à une ou des fonctionnalités nécessaires au bon fonctionnement de certaines applications ou à la qualité du service rendu à l'utilisateur.

218. Compte tenu du contexte concurrentiel particulier rappelé au paragraphe 197, l'Autorité souligne qu'une telle pratique pourrait être considérée comme relevant d'un traitement préférentiel si elle aboutissait à favoriser les applications propriétaires du fournisseur d'OS en dégradant la qualité des produits rivaux ou en accordant exclusivement, ou plus facilement, à ses applications une ressource ou une fonctionnalité leur permettant d'offrir un service que les concurrents ne pourraient fournir. À titre illustratif, tel pourrait être le cas si le fournisseur d'OS se réservait l'usage du GPS, lui permettant de bénéficier d'une géolocalisation fine pour ses seules applications propriétaires, ou s'il en facilitait l'accès pour son propre usage. De telles pratiques pourraient ériger des barrières à l'entrée et à l'innovation et réduire le choix d'applications disponibles pour les utilisateurs.

219. En deuxième lieu, l'Autorité souligne que ces dispositions à l'égard des fournisseurs d'OS semblent plus extensives que la disposition visant les éditeurs, laquelle paraît, par ailleurs, ambiguë puisqu'elle semble, d'une part, circonscrire le champ des permissions aux ressources sensibles et, d'autre part, donner l'initiative de la mise en œuvre d'un système de permission à l'éditeur.

220. En effet, la disposition visant les éditeurs à la section 5.5 indique que :

« *La CNIL encourage la pratique consistant à prévoir que l'application doit systématiquement obtenir la « permission » de l'utilisateur pour accéder à certaines ressources sensibles stockés sur le terminal (géolocalisation, carnet de contact, appareils photographiques et photographies/films, etc.), indépendamment des obligations légales résultant de l'article 82 de la loi Informatique et Libertés* »[128].

[127] Soulignements ajoutés.

[128] Soulignements ajoutés.

221. Sur cette disposition, l'Autorité invite la CNIL à clarifier l'articulation entre les dispositions des sections 5.5 et 8.3.1, et, en particulier, les responsabilités respectives des fournisseurs d'OS et des éditeurs ainsi que le périmètre des ressources concernées.

222. En troisième lieu, toujours s'agissant de la faculté du fournisseur d'OS de restreindre les ressources OS disponibles, la CNIL recommande aux fournisseurs d'OS, à la section 8.2.3, d'encourager les éditeurs à utiliser des fonctionnalités plus protectrices. À cet égard, la CNIL indique que le fournisseur d'OS « *devrait organiser la fin du support des fonctionnalités les plus problématiques, avec une période de transition suffisante pour permettre aux éditeurs de mettre à jour leurs applications* »[129].

223. S'agissant de cette recommandation, l'Autorité considère nécessaire de préciser ce qui est susceptible de constituer une fonctionnalité « *problématique* », l'imprécision de cette formulation laissant toute latitude au fournisseur d'OS de décider, sous couvert d'un objectif de protection de la vie privée, de ne plus donner accès à une fonctionnalité nécessaire au fonctionnement de certaines applications ou d'imposer une fonctionnalité moins fine.

224. L'Autorité invite également la CNIL à préciser les conditions de mise en œuvre de cette disposition, notamment s'agissant du délai de prévenance à respecter ainsi que de la nécessité de proposer une alternative satisfaisante.

En conclusion, ainsi qu'elle l'a indiqué aux paragraphes 215 et 221, l'Autorité invite la CNIL à clarifier les dispositions des sections 8.3.1 et 5.5 relatives à la mise en œuvre d'un système de permissions, s'agissant en particulier du périmètre des ressources concernées, de l'accessibilité des éditeurs aux ressources OS non soumises à une permission et des responsabilités respectives des fournisseurs d'OS et des éditeurs. Par ailleurs, l'Autorité invite la CNIL à préciser les conditions de mise en œuvre de la disposition de la section 8.2.3 relative à la fin du support des fonctionnalités les plus problématiques (voir paragraphes 223 et 224).

Sur l'ensemble de ces dispositions, et dans la mesure où l'usage des permissions ainsi préconisé par la CNIL ne résulte pas de la mise en œuvre directe de la réglementation applicable relative à la protection des données personnelles, l'Autorité appelle l'attention de la CNIL sur le fait que ses recommandations ne doivent pas conférer un pouvoir discrétionnaire trop important à certains acteurs verticalement intégrés, tels que les fournisseurs d'OS. Dans ce cadre, l'Autorité considère que la mise en œuvre de la protection de la vie privée ne doit pas entraver le dynamisme concurrentiel, ce qui suppose d'éviter que tout accès à une quelconque fonctionnalité du téléphone devienne soumis à permission, au détriment de la diversité de l'offre et de l'innovation. À tout le moins, l'Autorité invite la CNIL à préciser que le fournisseur d'OS est tenu d'appliquer des modalités de permissions proportionnées, objectives, transparentes et non-discriminatoires qui s'appliquent donc de façon uniforme à toutes les applications qu'elles soient préinstallées ou non, propriétaires ou non.

ii. Sur la transparence et la neutralité de la permission

225. Plusieurs acteurs entendus dans le cadre de l'instruction ont exprimé leur inquiétude sur le fait que les permissions pourraient conduire à un refus fréquent de l'utilisateur lorsque les demandes d'accès ne sont pas contextualisées. Certains acteurs soulignent également que certaines applications nécessitent obligatoirement, afin de fournir le service attendu par

[129] Soulignement ajouté.

l'utilisateur, d'accéder à certaines ressources de l'OS, ce qui devrait être clairement expliqué aux utilisateurs.

226. L'Autorité considère que la transparence de l'information est une condition nécessaire à l'exercice de la concurrence sur les marchés. En outre, l'Autorité souligne que la fourniture d'une information non neutre est susceptible de conduire à un traitement discriminatoire de certaines applications et, partant, de certains éditeurs, au détriment de la diversité de l'offre et de l'innovation.

À cet égard, l'Autorité considère que les utilisateurs devraient être clairement informés des finalités des permissions demandées, de manière neutre et contextualisée, afin de pouvoir exercer consciemment leur choix. La CNIL pourrait également préciser la distinction entre les permissions nécessaires et non nécessaires à la fourniture du service à l'utilisateur.

iii. Sur le renouvellement des demandes de permission

227. À la section 8.3.1, les recommandations de la CNIL prévoient que, « [p]*ar défaut,* [le fournisseur d'OS] *devrait permettre aux utilisateurs de n'autoriser l'accès qu'une seule fois ou uniquement quand l'application est active/en premier plan/utilisée, particulièrement pour les permissions les plus sensibles. Si l'application requiert une permission « à tout moment » (y compris quand l'application est fermée), l'information et le consentement de l'utilisateur devraient être renforcés* ».

228. Sur cette disposition, certains acteurs craignent que le fournisseur d'OS puisse mettre en place un dispositif conduisant à une réitération fréquente de la demande de permission, ce qui pourrait conduire à une dégradation de l'expérience de l'utilisateur.

229. L'Autorité considère que ceci pourrait nuire au bon fonctionnement concurrentiel du marché, notamment si un tel dispositif était mis en œuvre de façon discriminatoire par un acteur verticalement intégré qui ne l'appliquerait pas (ou pas de façon identique) à ses propres applications.

230. L'Autorité estime par conséquent que la CNIL devrait prendre en compte les impacts concurrentiels susceptibles de résulter de la mise en œuvre d'un dispositif prévoyant une réitération fréquente des demandes de permission. En outre, à défaut de définir clairement les « permissions les plus sensibles », une marge d'interprétation est laissée au fournisseur d'OS sur le champ de la mise en œuvre de cette disposition.

Dans ce cadre, l'Autorité invite la CNIL à prévoir (i) une définition claire des « *permissions les plus sensibles* » ; (ii) des garde-fous afin que l'expérience utilisateur ne soit pas dégradée par une multiplication des demandes ; et (iii) qu'il soit mis en œuvre un moyen aisé de revenir sur un choix de permission effectué préalablement (que ce soit en cas de refus ou d'accord).

iv. Sur la gestion des refus de permissions

231. À la section 8.3.1, la CNIL considère que « [l]*e fournisseur d'OS devrait décourager voire ne pas permettre de conditionner le lancement d'une application à l'obtention de permissions.* (…) *Il devrait permettre aux utilisateurs de décliner une permission sans que l'application soit automatiquement informée de ce refus. Par exemple, il devrait permettre*

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, etc. » [130].

232. Tout d'abord, l'Autorité estime que la concurrence et l'innovation sont fondées sur une transparence des marchés, laquelle doit être préservée, sinon encouragée. Ainsi légitimer *via* des recommandations le fait de ne pas informer l'application d'un refus de permission ou de fournir des données aléatoires n'est pas compatible avec une organisation transparente et efficace des marchés.

233. Cette disposition a d'ailleurs soulevé de nombreuses interrogations et craintes de la part des acteurs entendus.

234. Si quelques acteurs considèrent que cette disposition pourrait permettre d'empêcher que des éditeurs, notamment des opérateurs dominants, conditionnent l'utilisation d'une application à des permissions non nécessaires au fonctionnement de l'application – par exemple, à l'usage d'une fonctionnalité à des fins de monétisation de l'application – la plupart des acteurs entendus s'interrogent sur l'objet de cette disposition et s'inquiètent de ses modalités de mise en œuvre.

235. En premier lieu, plusieurs acteurs relèvent des contradictions entre cette disposition et la réglementation applicable en matière de protection des données personnelles, notamment ses principes de transmission de données fiables et précises, et de responsabilité.

236. En deuxième lieu, de nombreux acteurs redoutent que la mise en œuvre de cette disposition détériore la compétitivité des éditeurs (voire des développeurs), dans la mesure où l'envoi de données partielles ou erronées, sans que l'application en soit informée, est susceptible d'engendrer un dysfonctionnement de l'application et, au final, une insatisfaction de l'utilisateur. En outre, confrontés aux alertes de leur service client, les éditeurs et leurs développeurs pourraient engager en vain des ressources à la recherche des causes de ces dysfonctionnements. Par ailleurs, les éditeurs ne seraient plus en mesure de surveiller le nombre d'utilisateurs qui refusent les permissions, données utiles afin d'apporter des modifications à leurs applications. Enfin, la capacité de monétisation des applications des éditeurs pourrait en être affectée, et cela d'autant plus que la qualité du ciblage publicitaire serait altérée par l'envoi de données erronées – par exemple, de fausses informations concernant la géolocalisation, l'âge ou le sexe de l'utilisateur.

237. L'Autorité relève que l'ensemble de ces éléments pourrait porter atteinte à la compétitivité prix et hors prix des éditeurs et à leur capacité à financer leurs applications au moyen de la publicité. Il pourrait en résulter des barrières à l'entrée pour de nouveaux entrants potentiels.

238. En troisième lieu, les fournisseurs d'OS, offrant leurs propres services de publicité ciblée, pourraient être avantagés par le fait, d'une part, que les éditeurs tiers soient confrontés à une baisse de la qualité du ciblage publicitaire de leurs inventaires résultant de la réception de données vides, partielles ou erronées et, d'autre part, que les opérateurs verticalement intégrés puissent améliorer la qualité de leur propre ciblage par la collecte et le traitement de données supplémentaires.

239. En effet, l'Autorité considère que la généralisation des permissions est l'occasion pour les fournisseurs d'OS d'accroître le volume et le champ des données collectées par ces opérateurs. La disposition relative à la gestion du refus de permission pourrait, en créant un système d'intermédiation *via* le fournisseur d'OS, permettre à ce dernier de collecter, et ensuite d'utiliser à ses propres fins, des informations relatives aux réponses des utilisateurs

[130] Soulignements ajoutés.

qui relèvent uniquement de la relation avec l'éditeur. Notamment, les fournisseurs d'OS pourraient utiliser les informations collectées dans ce cadre pour s'octroyer un avantage concurrentiel soit en tant que magasins d'applications soit en tant qu'éditeurs.

240. À cet égard, l'Autorité rappelle que les opérateurs verticalement intégrés ne peuvent utiliser les informations des tiers pour leurs propres services pour lesquels ils ont été qualifiés de « contrôleur d'accès »[131]. Néanmoins, dans la mesure où il serait compliqué, en pratique, de savoir ce qui pourrait être fait de l'information collectée dans ce cadre, la généralisation du système des permissions ainsi que les dispositions relatives à la gestion des refus de permission par l'intermédiaire du fournisseur d'OS seraient susceptibles d'augmenter le risque d'utilisation de ces données par ce dernier pour son propre avantage.

241. L'Autorité souhaite également appeler l'attention de la CNIL sur le fait que les fournisseurs d'OS pourraient mettre en œuvre le dispositif de gestion des refus de façon discriminatoire, de façon à favoriser leurs propres applications. À titre illustratif, tel pourrait être le cas si les applications propriétaires de l'OS n'étaient pas soumises au même dispositif, ne recevant pas, sans en être informées, des données potentiellement vides, partielles ou erronées. Tel pourrait également être le cas si, les fournisseurs d'OS collectant nécessairement les données relatives aux refus de permission, ces derniers utilisaient ces données pour analyser les refus et les dysfonctionnements de l'application. En effet, compte tenu des effets potentiels sur la compétitivité des éditeurs, les applications tierces seraient désavantagées par rapport aux applications propriétaires.

242. Sur ces constats, l'Autorité considère que, outre le fait que cette disposition pourrait favoriser la mise en œuvre de potentielles pratiques anticoncurrentielles (par exemple, par la mise en œuvre du dispositif de gestion des refus de façon discriminatoire), la transmission sans en informer l'application, de données tronquées ou erronées, est à proscrire afin de ne pas perturber le fonctionnement des marchés en portant atteinte à leur transparence, en érigeant des barrières à l'entrée et à l'expansion et en renforçant les asymétries existantes.

Dans un souci de conformité avec les règles de concurrence, l'Autorité recommande que tout dispositif de gestion des demandes et refus de permissions soit mis en œuvre de façon objective, transparente et non discriminatoire.

Enfin, il serait souhaitable que la CNIL distingue les permissions nécessaires et facultatives à l'utilisation de l'application.

4. SUR LA SECTION CONCERNANT LES SDK

243. Comme exposé à la section I.A.1, le kit de développement logiciel désigne un ensemble d'outils utilisés pour le développement d'une application. Cette brique logicielle tierce, implantée dans l'application par l'ajout d'un code, permet de procéder à différentes opérations localement sur le terminal, ou en « appelant » des fonctionnalités offertes par des

[131] À cet égard, voir l'article 6(2) du DMA : « *Le contrôleur d'accès n'utilise pas, en concurrence avec les entreprises utilisatrices, les données, quelles qu'elles soient, qui ne sont pas accessibles au public, qui sont générées ou fournies par ces entreprises utilisatrices dans le cadre de leur utilisation des services de plateforme essentiels concernés ou des services fournis conjointement aux services de plateforme essentiels concernés, ou à l'appui de ceux-ci, y compris les données générées ou fournies par les clients de ces entreprises utilisatrices* ».

services en ligne tiers, le cas échéant en transmettant des informations personnelles issues du terminal (identifiant, adresse IP, configuration, etc.).

244. Le fournisseur de SDK peut être qualifié de sous-traitant, et donc être soumis au RGPD, lorsqu'il traite des données personnelles pour le compte de l'éditeur responsable du traitement. Il peut également être responsable de certains traitements de données personnelles effectués dans l'application s'il en détermine les finalités et les moyens.

245. Le secteur des SDK est caractérisé par une grande variété de fournisseurs, allant de petites *start-up* innovantes aux grandes plateformes numériques telles que Apple, Google ou encore Meta. De nombreux SDK sont offerts en *open-source*. Certains SDK – le plus souvent proposés par les grandes plateformes – sont considérés comme incontournables pour certains développeurs ou éditeurs. C'est par exemple le cas du SDK Firebase de Google pour l'analyse des données des utilisateurs et des Apple Pay SDK pour les systèmes de paiement.

246. S'agissant des recommandations de la section 7, concernant les bonnes pratiques à l'égard des fournisseurs de SDK ayant appelé de manière particulière l'attention de l'Autorité, la CNIL indique, à la section 7.1, que « *la prise en compte du respect de la vie privée doit commencer dès la phase de conception des SDK mis à disposition des éditeurs d'application*». Dans ce cadre, la CNIL fournit des recommandations aux fins de minimiser les données collectées (section 7.1.2) : « [l]*orsque le fournisseur d'OS ou un service tiers propose une fonctionnalité plus protectrice de la vie privée pour traiter certaines informations (par exemple une géolocalisation grossière au lieu d'une géolocalisation fine), qui semble plus pertinente en termes de minimisation de données, celle-ci devrait être mise en œuvre et les partenaires devraient être informés de la nécessité de mettre à jour leur SDK pour en tenir compte* ».

247. Cette disposition, qui ne découle pas directement du RGPD mais relève des bonnes pratiques suggérées par la CNIL, pourrait donner lieu à des interprétations divergentes. En effet, si certains acteurs interrogés interprètent cette recommandation comme la traduction directe du principe de minimisation[132], d'autres expriment leur inquiétude sur son interprétation possible.

248. En particulier, plusieurs acteurs entendus craignent que le fournisseur d'OS puisse imposer au fournisseur de SDK l'adoption d'une fonctionnalité, au motif qu'elle serait selon lui plus protectrice des données personnelles, indépendamment de la perspective du fournisseur du SDK. Sous couvert de l'application de cette recommandation, le fournisseur d'OS pourrait déterminer le catalogue des fonctionnalités disponibles pour les fournisseurs de SDK ainsi que leur finesse et, par ce moyen, imposer son interprétation de la conformité avec les règles relatives à la protection des données, celles-ci pouvant par ailleurs aller au-delà de la simple application du RGPD. Cette faculté emporterait un risque de mise en œuvre de potentielles pratiques anticoncurrentielles ainsi qu'une potentielle augmentation des barrières à l'entrée et à l'expansion. Tel pourrait être le cas si, par exemple, le fournisseur d'OS, acteur verticalement intégré le long de la chaîne de valeur et donc concurrent des éditeurs, altérait la qualité de services des applications concurrentes en leur fournissant désormais une fonctionnalité moins fine.

249. Par ailleurs, certains acteurs interrogés ont relevé l'absence de toute mention relative à un délai acceptable de mise à jour, alors que la mise à jour de SDK peut prendre du temps et

[132] Ce principe implique de retenir la fonctionnalité la plus protectrice à la condition qu'elle permette de satisfaire la finalité du service rendu par l'application, sans détérioration de la qualité de ce service.

nécessiter des tests préalables aux mises à jour effectives. La référence à un « service tiers » dans la recommandation est également considérée peu claire et comme devant être précisée.

250. L'Autorité constate que la formulation de cette disposition est ambiguë et pourrait conduire à des interprétations divergentes, en particulier en ce qui concerne le rôle du fournisseur d'OS. L'Autorité considère notamment que, dans le cas où la recommandation de la CNIL confierait au fournisseur d'OS un pouvoir supplémentaire qui ne découle pas directement du RGPD, ce dernier pourrait l'utiliser pour fausser la concurrence entre les éditeurs d'applications mobiles lorsque cette utilisation n'est pas faite de manière objective, proportionnée, transparente et non discriminatoire.

L'Autorité estime que la disposition de la section 7.1.2 mérite *a minima* d'être clarifiée si elle devait demeurer sous sa forme actuelle. Néanmoins, elle appelle la CNIL à en modifier le principe notamment en invitant les fournisseurs d'OS à informer les fournisseurs de SDK de l'existence de nouvelles fonctionnalités et de la possibilité de mettre à jour leur SDK. Ainsi, au lieu d'un devoir d'adaptation automatique du SDK, il conviendrait de prévoir un devoir d'information de la part de l'OS et d'examen de la part du SDK.

5. SUR LA SECTION CONCERNANT LES FOURNISSEURS DE MAGASINS D'APPLICATIONS MOBILES

251. Dans son projet, la CNIL confère aux fournisseurs de magasins d'applications un rôle important en matière de protection de la vie privée.

252. À titre liminaire et comme indiqué ci-avant (section II.C.1.b), l'Autorité relève que ce rôle ainsi accordé aux fournisseurs de magasins d'applications ne résulte pas d'obligations conférées par la réglementation en vigueur relative à la protection des données personnelles et de la vie privée.

253. En effet, la CNIL précise dans son projet que « *le fournisseur du magasin d'applications ne sera généralement pas responsable des traitements mis en œuvre au sein des applications elles-mêmes*[133] ». Cependant, la CNIL remarque que le fournisseur du magasin d'applications peut avoir, de par « *ses choix de conception, la clarté des informations qu'il propose et sa capacité à contrôler les applications qu'il met à disposition* », « *un fort impact sur les traitements de données personnelles mis en œuvre via les applications* »[134]. À ce titre, la CNIL considère « *souhaitable que le fournisseur du magasin d'applications présente une information claire sur les traitements susceptibles d'être mis en œuvre au sein des applications distribuées et qu'il mette en œuvre des processus participant à assurer la conformité aux législations en vigueur des applications publiées* »[135].

254. La CNIL recommande en particulier aux fournisseurs de magasins d'applications de mener une analyse des applications soumises par les éditeurs en vue d'être référencées dans leur magasin, de mettre en œuvre des processus transparents de revue des applications qui intègrent la vérification de règles élémentaires de protection des données et d'informer les utilisateurs afin de leur permettre d'exercer leurs droits plus facilement.

---

[133] Projet de recommandation relative aux applications mobiles, section 9, page 85.

[134] *Ibidem*.

[135] *Ibidem*.

255. Ces recommandations reflètent la volonté de la CNIL d'améliorer la protection de la vie privée par la mise en œuvre de bonnes pratiques sur l'ensemble de la chaîne de valeur des écosystèmes mobiles, y compris à la maille des fournisseurs de magasins d'applications.

256. L'Autorité constate à cet égard que les magasins d'applications App Store et Play Store ont progressivement mis en œuvre des conditions d'accès intégrant des règles relatives à la protection de la vie privée des utilisateurs[136].

257. Cependant, compte tenu du contexte concurrentiel relatif au secteur des applications mobiles, l'Autorité souhaite appeler l'attention de la CNIL sur la nécessité de veiller à ce que ses recommandations relatives aux fournisseurs de magasins d'applications ne portent pas atteinte à la concurrence qui peut s'exercer entre les acteurs présents aux différents maillons de cette chaîne de valeur ou à l'égard d'entrants potentiels. En effet, comme indiqué à la section I.A.2, les deux principaux magasins d'applications sont fournis par deux grands acteurs verticalement intégrés au sein de la chaîne de valeur des applications mobiles, Apple et Google, qui ont été désignés contrôleur d'accès au sens du DMA, notamment pour leurs magasins d'applications, et sont susceptibles de détenir une position dominante sur certains marchés de cette chaîne de valeur[137].

258. À cet égard, comme indiqué notamment à la section I.A.2, plusieurs autorités nationales ont déjà soulevé des préoccupations de concurrence à l'égard des magasins d'applications de Google et Apple dans le cadre de rapports dédiés à l'écosystème mobile[138] ou de l'examen d'affaires relatives à des dossiers antitrust.

259. Par exemple, dans sa décision du 18 juillet 2018, confirmée par l'arrêt du Tribunal de l'Union du septembre 2022, la Commission a sanctionné Google pour avoir notamment

---

[136] Ainsi que le rapporte par exemple le *United States Department of Commerce*, les développeurs d'applications doivent notamment s'engager à ce que les applications (ainsi que tous les outils utilisés pour créer et maintenir une application) soient utilisées de manière à protéger les données des utilisateurs. Selon ce rapport, « *Apple affirme qu'elle rejette environ 40 % des applications proposées, souvent en raison de problèmes logiciels ou de bogues, ou parce qu'elles compromettraient la vie privée ou la sécurité des utilisateurs. Apple affirme que la plupart des applications rejetées sont finalement intégrées dans le magasin d'applications mobiles*. (…) *En 2021, Google affirme avoir empêché "1,2 million d'applications violant les règles" d'être lancées sur le Google Play Store, "banni 190 000 mauvais comptes et fermé environ 500 000" comptes de développeurs inactifs ou abandonnés, selon l'entreprise. En outre, Google utilise des mesures de protection de la sécurité telles que Google Play Protect, qui analyse "plus de 125 milliards d'applications chaque jour" à la recherche d'applications potentiellement dangereuses, d'exploitation de réseau, de phishing et de logiciels malveillants* ». (*Competition in the mobile application ecosystem*, United States Department of Commerce, février 2023, page 29 (traduction libre de l'Autorité).).

[137] Par exemple, dans sa décision Google Android du 18 juillet 2018 (Décision C(2018) 4761), la Commission européenne a conclu que Google occupe une position dominante sur les marchés des systèmes d'exploitation mobiles intelligents sous licence et des boutiques d'applications en ligne pour le système d'exploitation mobile Android**.**

[138] Le rapport précité de la CMA du 10 juin 2022 s'interroge notamment sur les conditions d'accès des éditeurs aux magasins d'applications de Google et d'Apple, en particulier dans le cadre de leur processus de revue des applications, et, s'agissant de la face utilisateurs des magasins d'application, à la présentation des applications, en particulier l'architecture des choix retenue. Dans ce même rapport, la CMA s'est également inquiétée du fait que les arguments relatifs à la sécurité et à la vie privée des utilisateurs pourraient justifier des décisions qui servent également à nuire à la concurrence ou à limiter le choix des consommateurs.

Voir également les rapports "*Competition in the mobile application ecosystem*", Department of Commerce, février 2023 et « *Market Study Report on Mobile OS and Mobile App Distribution* », The Japan Fair Trade Commission (JFTC), February 2023.

abusé de sa position dominante[139] en imposant aux fabricants d'appareils mobiles des restrictions contractuelles anticoncurrentielles insérées dans des « accords de distribution » obligeant ces fabricants à préinstaller les applications de recherche générale (Google Search) et de navigation (Chrome) pour pouvoir obtenir de Google une licence d'exploitation de sa boutique d'applications Play Store.

260. La nécessité de tenir compte du contexte concurrentiel propre au secteur afin d'apprécier l'impact des recommandations de la CNIL est également partagée par la plupart des acteurs interrogés. Selon ceux-ci, certaines dispositions peuvent en effet conduire à renforcer les asymétries existantes, au profit de ces deux grands acteurs verticalement intégrés. Ces acteurs ont également relevé différentes préoccupations concernant le rôle conféré par certaines recommandations de la CNIL aux fournisseurs de magasins d'applications (voir section II.C.1 consacrée aux remarques préalables sur les problématiques concurrentielles).

261. L'Autorité partage ces préoccupations et souhaite, au-delà des remarques générales faites jusqu'ici, appeler l'attention de la CNIL sur plusieurs dispositions spécifiques de la section consacrée aux fournisseurs de magasins d'applications.

a) Sur la collecte d'informations et l'analyse des applications relatives à la conformité

262. En introduction de la section 9.1 des recommandations relatives aux fournisseurs de magasins d'applications, la CNIL indique que « [l]*ors du processus de revue des applications dont les éditeurs sollicitent la publication au sein du magasin d'applications, le fournisseur du magasin a la possibilité de procéder à la collecte d'informations et à l'analyse de l'applicatif proposé afin de favoriser le respect des droits des utilisateurs finaux* »[140].

263. À la section 9.1.1 intitulée « *Centraliser et analyser les données relatives à la conformité* », la CNIL précise que « *le fournisseur du magasin d'applications peut demander la transmission de la documentation préexistante constituée par l'éditeur afin d'encourager les bonnes pratiques en termes de protection des données personnelles et renforcer la transparence pour les utilisateurs* ». Dans cette même section, elle recommande par ailleurs au fournisseur du magasin d'applications « *de solliciter a minima les informations suivantes*[141] :

---

[139] Plus précisément, dans sa décision Google Android du 18 juillet 2018 précitée, la Commission conclut que Google occupe depuis 2011 une position dominante: i) sur le marché mondial (à l'exception de la Chine) des systèmes d'exploitation mobiles intelligents sous licence; ii) sur le marché mondial (à l'exception de la Chine) des boutiques d'applications Android; et iii) sur chacun des marchés nationaux des services de recherche générale dans l'EEE.

Dans un arrêt du 14 septembre 2022 précitée, le Tribunal de l'Union européenne a par ailleurs souligné que, « *si les marchés pertinents sont présentés de manière distincte dans la décision attaquée, ils ne sauraient toutefois être artificiellement dissociés dans la mesure où ils présentaient tous des aspects complémentaires dûment évoqués par la Commission* ».

[140] Soulignement ajouté.

[141] Soulignements ajoutés.

- *les catégories de données collectées et les finalités poursuivies pour chacun des traitements,*
- *les tiers qui ont accès aux données ou qui sont susceptibles d'y avoir accès, ce qui peut inclure la liste des fournisseurs de SDK utilisés,*
- *la liste exhaustive des permissions système demandées par l'application, comprenant leur nature obligatoire ou optionnelle, ainsi que les finalités pour lesquelles celles-ci sont demandées, telles qu'elles seront présentées à l'utilisateur lors de l'usage de l'application,*
- *le pays dans lequel les données seront stockées et traitées,*
- *un historique des mises à jour, incluant les notes de mises à jour*. »

264. Certains acteurs interrogés dans le cadre de l'instruction accueillent positivement ces dispositions dans la mesure où ils les estiment favorables à une meilleure sécurité de l'utilisateur.

265. Néanmoins, certains de ces acteurs ont relevé les imprécisions de ces dispositions et, plus largement, s'inquiètent du fait que la CNIL souhaite confier aux fournisseurs de magasins d'applications un rôle particulier de collecte d'informations et de contrôle de la conformité.

266. Sur ce point, l'Autorité souhaite plus particulièrement appeler l'attention de la CNIL sur (i) les risques relatifs à la communication d'informations commercialement sensibles, (ii) les conséquences potentielles d'un processus de revue intégrant une analyse de la conformité qui serait opaque et rendue plus complexe, ce qui pourrait engendrer un risque de rejets injustifiés d'applications de tiers ou de délais dans le processus de revue ainsi que (iii) sur la charge qu'une analyse de la conformité pourrait représenter pour un fournisseur de magasins d'applications.

i. Sur la communication d'informations commercialement sensibles

267. La plupart des acteurs interrogés se sont inquiétés de ce que la liste fournie dans le cadre de cette disposition soit une liste *a minima* et sans précision du niveau de détail attendu des informations. Certains acteurs ont également relevé que l'objectif visant à « *favoriser le respect des droits des utilisateurs finaux* » reste vague, laissant une marge d'interprétation aux fournisseurs de magasins d'applications pour déterminer les informations susceptibles de relever de cet objectif. Ces imprécisions pourraient permettre aux fournisseurs de demander des informations commercialement sensibles, sous couvert de cette disposition.

268. Par exemple, certains acteurs craignent que l'on puisse demander aux éditeurs les finalités fines de traitement des données collectées. Un acteur du secteur a également souligné que *« la documentation préexistante de l'éditeur* », mentionnée dans cette disposition, pouvait comprendre des informations détaillées à ne pas mettre dans les mains de concurrents ou d'autres acteurs du marché, par exemple l'analyse d'impact réalisée en interne concernant l'intérêt légitime, mise à disposition de la seule autorité de contrôle sur demande.

269. Dans cette perspective, les acteurs craignent que les plateformes verticalement intégrées puissent retirer un avantage concurrentiel des informations ainsi collectées par le biais de leurs magasins d'applications.

270. Enfin, un acteur a indiqué que, dans la mesure où la protection des données est susceptible d'être considérée comme un paramètre de concurrence, des échanges d'informations confidentielles sur ce paramètre de concurrence entre le magasin d'applications, qui édite

lui-même des applications, et les éditeurs d'applications concurrentes tierces, pourraient être qualifiés d'échanges d'informations sensibles entre concurrents.

271. L'Autorité partage ces inquiétudes. Compte tenu, là encore, du contexte concurrentiel rappelé au paragraphe 257, la collecte d'informations et l'analyse des applicatifs de leurs concurrents par des opérateurs verticalement intégrés pourraient leur permettre d'accéder à des informations potentiellement utiles pour améliorer leurs propres applications ou pour lancer de nouvelles applications concurrentes et de renforcer l'asymétrie d'information à leur profit.

272. Une telle pratique serait susceptible de poser des problèmes concurrentiels si elle était mise en œuvre par des acteurs en position dominante. Par ailleurs, des échanges d'informations sensibles entre concurrents seraient susceptibles de constituer des pratiques horizontales anticoncurrentielles entrant ainsi dans le champ de l'article 101 du TFUE (ou de l'article L. 420-1 du code de commerce).

Sur ce point, l'Autorité invite la CNIL à préciser (i) que les données sont collectées auprès des éditeurs sur une base déclarative et que les recommandations n'impliquent pas que les fournisseurs de magasins d'applications ont la responsabilité d'en vérifier l'exactitude ; et (ii) que les données transmises aux magasins d'applications doivent exclure toute information commercialement sensible.

En outre, la CNIL pourrait également utilement rappeler les obligations qui incombent à Google et Apple en tant que « contrôleurs d'accès » sur les magasins d'applications, notamment l'interdiction d'utiliser les données des entreprises utilisatrices concurrentes, collectées dans le cadre de l'activité relevant du DMA pour un usage sur un autre marché, prévue à l'article 6(2) du DMA[142].

ii. Sur l'analyse de conformité

273. Si les fournisseurs de magasins d'applications procèdent déjà, dans le cadre de leur processus de revue, à des analyses tenant compte d'une appréciation de la conformité des applications, plusieurs acteurs entendus craignent que, sous couvert de la mise en œuvre des recommandations de la CNIL, les dispositions concernées viennent entériner des processus de revue qui leur posent déjà des difficultés. Plusieurs acteurs interrogés soulignent notamment le manque de transparence des règles actuelles des magasins d'applications, le rejet fréquent des applications lors de leur première soumission, le manque d'explications sur les causes de rejet ou encore le délai aléatoire pour obtenir une acceptation. Ces réponses font écho aux préoccupations déjà soulevées par différentes autorités de concurrence dans le cadre de leur analyse de la situation concurrentielle dans les écosystèmes mobiles (voir notamment section I.A.2).

274. S'agissant plus particulièrement de l'appréciation de la conformité à la réglementation relative à la protection des données personnelles et de la vie privée dans le cadre du processus de revue, un acteur du secteur rapporte que le rejet d'une application peut reposer sur un malentendu relatif à la non-conformité d'une application à cette réglementation, en raison

[142] L'article 6(2) du DMA précise en effet : « *le contrôleur d'accès n'utilise pas, en concurrence avec les entreprises utilisatrices, les données, quelles qu'elles soient, qui ne sont pas accessibles au public, qui sont générées ou fournies par ces entreprises utilisatrices dans le cadre de leur utilisation des services de plateforme essentiels concernés ou des services fournis conjointement aux services de plateforme essentiels concernés, ou à l'appui de ceux-ci, y compris les données générées ou fournies par les clients de ces entreprises utilisatrices.* »

de différences d'interprétation entre les parties. Le rejet de l'application et la nécessité de fournir des explications afin de dissiper ce malentendu engendrent des délais et des coûts pour l'éditeur.

275. Par ailleurs, certains acteurs redoutent une complexification à venir du processus de revue et les conséquences, en termes de délais et de coûts, qui pourraient en résulter pour les éditeurs et développeurs. Par exemple, certains acteurs s'interrogent sur la possibilité pour les fournisseurs de magasins d'applications de demander, sous couvert de cette disposition, des informations supplémentaires pour la revue des applications. En l'absence de précisions relatives tant aux informations susceptibles d'être exigées que des critères qui seraient potentiellement mis en place par les fournisseurs de magasins d'applications dans le cadre de l'analyse de conformité recommandée par la CNIL, certains acteurs redoutent des risques accrus de rejet de leur application, allongeant les délais de référencement de leur application ou engendrant un blocage de la mise à jour d'une application déjà référencée dans le magasin.

276. Enfin, plusieurs acteurs entendus considèrent que les fournisseurs de magasins d'applications ne seraient pas en mesure de vérifier que les informations fournies dans la politique de confidentialité de l'éditeur correspondent aux collectes et retraitements de données effectués pour les finalités désignées dans le cadre de l'utilisation de son application, et, en particulier, d'auditer ces traitements. Seuls les éditeurs disposeraient d'un accès direct aux informations et au contexte requis pour évaluer leurs traitements des données, dont la plupart se déroulent sur les serveurs des développeurs.

277. Sur ces constats et compte tenu du contexte particulier du secteur concerné, l'Autorité souhaite appeler l'attention de la CNIL sur le fait que certaines pratiques relatives à la mise en œuvre d'un processus de revue opaque et complexe seraient susceptibles, dans certaines conditions, d'être qualifiées d'abus de position dominante.

278. À titre illustratif, un fournisseur de magasins d'applications pourrait être tenté de mettre en œuvre un processus de revue des applications de façon non proportionnée et/ou discriminatoire, sous couvert d'un objectif d'analyse des données relatives à la conformité, par exemple, en allongeant les délais de revue des applications tierces afin d'en retarder le lancement ou la mise à jour ou en mettant en œuvre des critères de conformité disproportionnés. Le cas échéant, une telle pratique pourrait engendrer des coûts pour les éditeurs tiers et constituer des barrières à l'entrée pour de nouveaux éditeurs et/ou développeurs entrants, par exemple sur des marchés où le fournisseur de magasins d'application est déjà présent en tant qu'éditeur.

279. Toujours à titre illustratif, la référence à une « *possibilité* » de procéder à la collecte d'informations et à l'analyse de l'applicatif – et non à une obligation – ainsi que l'imprécision des critères potentiels d'analyse de la conformité, ouvrent la voie à un potentiel traitement discriminatoire des applications. En particulier, la recommandation ainsi formulée laisse au fournisseur de magasins d'applications la latitude de décider, selon des critères qui lui sont propres, dans quels cas la collecte des informations et l'analyse sont requises et dans quels cas elles ne le sont pas.

280. En conclusion sur cette disposition, et comme elle l'a indiqué dans la section II.C.1.b), l'Autorité rappelle qu'un opérateur, y compris en position dominante, est libre d'édicter les règles qu'il estime utiles pour conditionner l'accès à ses biens ou ses services, sous réserve que leur mise en œuvre n'ait pas pour objet ou pour effet de restreindre la concurrence. Cependant, l'Autorité appelle l'attention de la CNIL sur le fait que ses recommandations ne doivent pas avoir pour effet de déléguer aux fournisseurs de magasins d'applications ses missions de régulation, dans la mesure où cela pourrait aboutir à distordre la concurrence sur

les marchés en cause ou à conférer un pouvoir de marché supplémentaire à ces acteurs verticalement intégrés.

Pour ces raisons, l'Autorité invite la CNIL à (i) circonscrire sa recommandation relative à l'analyse de conformité aux obligations particulières de ces acteurs résultant des réglementations en vigueur[143] ; (ii) préciser qu'à tout le moins, ces vérifications devraient être réalisées pour l'ensemble des applications soumises à la revue des magasins et aux applications préinstallées, y compris les applications propriétaires ; et (iii) préciser l'importance de mettre en œuvre un processus de revue garantissant des conditions d'accès transparentes, équitables et non discriminatoires sur la base de critères proportionnés et prévoir des formes de dialogue entre les parties, et tout particulièrement un mécanisme de règlement des différends.

À ce titre, l'Autorité rappelle que de telles obligations semblent relever de l'article 6(12) du DMA applicable aux contrôleurs d'accès[144].

iii. Sur les potentielles barrières à l'entrée et à l'expansion pour les magasins d'applications alternatifs

281. Comme exposé dans la section I.A.2, l'App Store est, à date, le seul magasin d'applications autorisé par Apple sur les terminaux mobiles d'Apple, et le Play Store est le principal magasin d'applications utilisé sur les terminaux mobiles équipés du système d'exploitation Android. La concurrence exercée par les magasins de certains fabricants mobiles (tel que Samsung) ou par les magasins en open source (tel que F-Droid) demeure faible.

282. Selon un acteur du secteur, les magasins en *open source* sont assimilables à des annuaires d'applicatifs. Ils ne procèdent pas à une analyse des applicatifs dans le cadre d'un processus de revue mais se fondent sur une revue de code par la communauté.

283. L'Autorité relève, à l'instar de certains acteurs, que les recommandations de la CNIL ne font pas référence à cette diversité de fournisseurs de magasins d'applications. De plus, l'Autorité souligne que la mise en œuvre de contrôles de conformité tels que suggérés par la CNIL dans ses recommandations est susceptible de représenter une contrainte et une charge potentiellement importante pour les magasins alternatifs et, le cas échéant, d'entraver l'émergence et le développement de ces magasins.

Sur ces constats, l'Autorité invite la CNIL à préciser les modalités d'application pour les magasins d'applications alternatifs et de petite taille, actuels et potentiels, afin que les recommandations ne représentent pas une contrainte à l'entrée ou à la survie pour ces derniers.

---

[143] Des obligations relatives à l'analyse de la conformité peuvent notamment résulter du règlement (UE) 2022/2065 du Parlement européen et du Conseil du 19 octobre 2022 relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE (règlement sur les services numériques ou « *Digital Service Act* » (DSA)).

[144] L'Article 6(12) du DMA dispose que « [l]*e contrôleur d'accès applique aux entreprises utilisatrices des conditions générales d'accès équitables, raisonnables et non discriminatoires à ses boutiques d'applications logicielles, moteurs de recherche en ligne et services de réseaux sociaux en ligne énumérés dans la décision de désignation conformément à l'article 3, paragraphe 9. À cette fin, le contrôleur d'accès publie des conditions générales d'accès, comportant notamment un mécanisme de règlement extrajudiciaire des litiges.* »

b) Sur la possibilité pour les acteurs verticalement intégrés d'imposer leur interprétation de la conformité avec la réglementation européenne

284. Dans la section 9.2 de son projet, la CNIL insiste sur l'importance, pour les fournisseurs de magasins d'applications, d'agir avec la plus grande transparence et de faciliter les démarches des éditeurs tout au long du processus de publication des applications. Si l'Autorité partage cet objectif, qu'elle estime positif sur le plan concurrentiel (ii), elle souhaite également appeler l'attention de la CNIL sur les risques concurrentiels liés à la possibilité pour des acteurs verticalement intégrés d'imposer, sous couvert de l'application de ses recommandations, leur interprétation de la conformité par la délivrance de conseils (section 9.2.1) (i).

i. Sur les recommandations relatives à la délivrance de conseils relatifs à la conformité avec les règles européennes de protection des données

285. À la section 9.2.1 des recommandations relatives aux fournisseurs de magasins d'applications, la CNIL recommande que :

« *Pour les applications d'éditeurs installés hors de l'Union européenne mais visant le marché européen, il devrait être demandé à l'éditeur si l'application traite des données personnelles. Dans ce cas :* (…)

- *la fourniture d'un point de contact pour les utilisateurs de l'Union européenne souhaitant exercer leurs droits devrait être exigée,*
- *il devrait être demandé à l'éditeur de soumettre dans le processus de revue les informations clés de protection des données : finalités poursuivies, données traitées, modalités d'exercice des droits, durées de conservation,*
- *des conseils sur la mise en conformité avec les règles européennes de protection des données devraient être délivrés à l'éditeur.*

Il serait utile que les magasins d'applications refusent les applications qui ne sont pas en mesure de fournir les éléments ci-dessus.

Par ailleurs, le fournisseur de magasins d'applications pourrait utilement proposer aux utilisateurs un mécanisme de signalement des applications ne respectant pas les règles ci-dessus, pouvant conduire à une exclusion de l'application du magasin » [145].

286. À titre liminaire, de nombreux acteurs interrogés soulignent les effets positifs, en particulier pour les petits acteurs, d'une facilitation de l'accès aux informations relatives à la réglementation sur la protection de la vie privée.

287. Si certains acteurs précisent que les informations fournies par le magasin d'applications devraient être limitées à une synthèse des règles applicables, voire à des renvois vers des documentations institutionnelles, d'autres considèrent utile que les petits acteurs puissent être aidés dans la compréhension de ces règles et dans leur mise en œuvre. En réduisant les barrières à l'entrée pour les éditeurs, la communication d'informations, voire de conseils, pourrait ainsi avoir un effet pro-concurrentiel.

288. Cette recommandation pourrait néanmoins soulever plusieurs difficultés en pratique.

289. Plusieurs acteurs relèvent que cette disposition emporte des risques pour les acteurs en termes de responsabilité. D'une part, les éditeurs demeurent les seuls responsables de

[145] Soulignements ajoutés.

traitement au sens du RGPD alors même qu'ils pourraient être dans l'obligation de suivre des conseils inadaptés, voire erronés, prodigués par un fournisseur de magasins d'applications. D'autre part, les fournisseurs de magasins d'applications pourraient voir leur responsabilité engagée en cas de conflit avec un éditeur sanctionné par l'autorité compétente pour avoir mis en œuvre des conseils non conformes à la réglementation applicable.

290. Au-delà de ces difficultés, plusieurs acteurs s'inquiètent du fait que cette disposition confère un rôle de régulateur au fournisseur de magasins d'applications, lequel pourrait ainsi imposer son interprétation de la conformité avec les règles européennes de protection des données – à tout le moins à l'ensemble des applications d'éditeurs installés hors de l'UE visant le marché européen. À cet égard, certains acteurs relèvent que les dispositions précitées au paragraphe 285 concernant le refus d'applications par les magasins d'applications d'une part, et la mise en œuvre d'un mécanisme de signalement d'autre part, sont peu claires dans leur formulation et leur champ d'application. En conséquence, ces dispositions pourraient être interprétées comme prévoyant l'application de sanctions en l'absence de mise en œuvre des conseils prodigués par les fournisseurs de magasins d'applications, ce qui renforcerait la contrainte que ces derniers pourraient exercer sur leurs concurrents.

291. Sur cette disposition, l'Autorité considère que la recommandation de délivrance de conseils d'ordre juridique est susceptible de conférer un rôle trop prescriptif au fournisseur de magasins d'applications, lui permettant le cas échant d'imposer son interprétation de la conformité. En outre, la possibilité pour ce fournisseur d'exclure des applications en cas de non-respect de ses conseils confèrerait auxdits conseils un caractère obligatoire pour les éditeurs souhaitant faire référencer leur application dans ce magasin. Dans la mesure où les principaux fournisseurs de magasins d'applications sont des acteurs verticalement intégrés, ce rôle de conseil les placerait dans une position de juge et partie.

292. À titre illustratif, ces acteurs pourraient être tentés d'utiliser ce rôle de conseil pour décourager l'entrée d'éditeurs concurrents, affaiblir leur compétitivité ou freiner l'innovation, par exemple en les encourageant à adopter des normes excessives et coûteuses au regard des exigences de la réglementation sur la protection de la vie privée ou en les incitant à renoncer à l'adoption de SDK innovants ou nécessaires à la fourniture d'un service différencié ou de meilleure qualité.

Sur ces constats, l'Autorité invite la CNIL à préciser la disposition précitée en limitant l'information communiquée par les fournisseurs de magasins d'applications relative à la réglementation européenne sur la protection des données personnelles et de la vie privée à la fourniture (i) de synthèses de certaines dispositions réglementaires renvoyant aux textes applicables (ii) de documents publiés par les autorités compétentes, en particulier la CNIL, (iii) d'un lien vers les sites internet de ces autorités ou (iv) des points de contact de ces autorités.

Cette information pourrait utilement être communiquée à l'ensemble des éditeurs et développeurs dont les applications mobiles visent les utilisateurs situés en France et sur le territoire de l'Union européenne (i) en clarifiant la disposition relative au refus d'accès et notamment en précisant les éléments pouvant motiver un refus, ainsi qu'en prévoyant des conditions de recours et de règlement de différends pour les éditeurs des applications concernées, ainsi que le prévoit le DMA à son article 6(12) ; et (ii) en indiquant que si un magasin d'applications peut utilement proposer un mécanisme de signalements, ce mécanisme devrait avoir une portée limitée, respecter les modalités décrites dans le règlement sur les services numériques (ou « *Digital Services Act* » (DSA)) et réserver à la CNIL l'exclusivité de l'interprétation des textes applicables.

ii. Sur les recommandations de transparence du processus de revue des applications

293. À la section 9.2.2, la CNIL recommande aux fournisseurs de magasins d'applications d'exposer clairement leurs attentes et les processus mis en œuvre.

294. Plus précisément, la CNIL indique que « *dans la mesure du possible, il serait utile pour l'ensemble des acteurs que les fournisseurs de magasin d'applications s'assurent de la clarté des exigences imposées aux applications candidates en termes de sécurité et de vie privée* ».

295. Par ailleurs, la CNIL fournit une liste d'informations à communiquer aux éditeurs, à titre de bonnes pratiques :

- *« La mise à disposition d'une documentation complète concernant les points d'exigence étudiés ;*
- *Pour chacune de ces exigences, la publication d'exemples concrets de comportements problématiques, et de solutions pour y remédier,*
- *La mise à disposition d'une description précise du processus de validation, des étapes de vérification et des temporalités associées à chaque étape, y compris pour les différents processus de remédiation en cas de rejet,*
- *En cas de mise à jour des règles applicables, une communication proactive aux éditeurs concernant celles-ci, en allouant une période raisonnable pour leur prise en compte. Si ces mises à jour ont vocation à provoquer le rejet de solutions précédemment acceptées, des exemples de techniques de remédiations peuvent également être publiés ».*

296. À la section 9.2.3, la CNIL recommande aux fournisseurs de magasins d'applications de « *s'assurer qu'ils mettent à disposition des outils adéquats pour la gestion du processus de publication et de résolution de rejets* ».

297. À la section 9.2.4, la CNIL recommande aux fournisseurs de magasins d'applications d'être transparents sur les causes de rejet et les voies de recours. Plus précisément, la CNIL recommande à ces acteurs de s'assurer que les raisons de refus et suspensions sont suffisamment compréhensibles, en préconisant :

« *Une communication transparente avec les éditeurs d'applications mobiles lors de l'application des critères de validité de publication devrait être assurée. Les causes du rejet et le processus de recours mobilisable par l'éditeur devraient être indiqués de manière claire et précise.*

En particulier, les raisons du refus et les méthodes de remédiation proposées devraient être spécifiées dans la documentation.

Si une faille de sécurité est détectée, et en particulier si cela peut mener à la désactivation de l'application ou à une communication aux utilisateurs finaux, l'éditeur devrait en être informé de manière renforcée.

Une communication avec les éditeurs d'applications dans leur langue est souhaitable ».

298. L'Autorité accueille favorablement ces recommandations qui vont dans le sens d'une amélioration de la transparence, dans un contexte où plusieurs autorités de concurrence ont relevé des préoccupations de concurrence relatives au manque de transparence concernant les processus de revue des applications, notamment de Google et Apple (voir section I.A.2).

À cet égard, l'Autorité a déjà pu rappeler l'importance de mettre en œuvre des règles d'accès transparentes, objectives, non discriminatoires et proportionnées à l'objectif poursuivi[146].

Sur ce point, la CNIL pourrait en outre utilement rappeler aux acteurs, à titre d'information, que le DMA prévoit en son article 6(12) que les contrôleurs d'accès appliquent des conditions générales d'accès à leurs magasins d'applications et mettent à disposition des entreprises partenaires un mécanisme d'arbitrage pour régler les différends éventuels sur les conditions d'accès.

c) Sur l'information des utilisateurs et la fourniture d'outils de signalement et d'exercice des droits

299. À la section 9.3, la CNIL préconise, au titre de bonnes pratiques, d'afficher certaines informations dans les pages de chaque application, à destination des utilisateurs.

300. L'Autorité accueille favorablement la volonté de la CNIL de favoriser une meilleure information des utilisateurs, laquelle est, au-delà du prisme du droit des utilisateurs, favorable à l'exercice d'une meilleure dynamique concurrentielle. En effet, la réduction de l'asymétrie d'informations entre offreurs et demandeurs par la diffusion d'une information objective et plus complète, permet aux utilisateurs de mieux comparer les produits et services offerts afin de répondre à leurs besoins et stimule la concurrence entre les entreprises.

301. Toutefois, plusieurs acteurs interrogés ont fait part de leurs craintes relatives à certaines dispositions de cette section.

302. Dans ce qui suit, l'Autorité souhaite appeler plus particulièrement l'attention de la CNIL sur les dispositions relatives aux modalités de financement des éditeurs et à la mise en œuvre de filtrages ou scores concernant des critères relatifs à la protection de la vie privée.

Sur l'affichage des informations relatives aux modalités de financement des applications

303. À la section 9.3.1, la CNIL indique que « [d]*ans le contexte des interfaces mobiles, il peut être complexe de rendre compréhensible l'ensemble de ces informations. Afin d'en faciliter la lecture, l'utilisation de représentations graphiques, par exemple l'utilisation d'icônes et de tableaux, en choisissant ceux-ci de manière à souligner les éléments ayant le plus d'impact en termes de protection de la vie privée, devrait être privilégiée. L'information mise à disposition pourrait notamment comprendre des informations relatives aux modalités de financement de l'application, notamment lorsque celui-ci repose directement sur une réutilisation des données personnelles de l'utilisateur pour d'autres finalités. Le cas échéant, l'information devrait être présentée de manière neutre et contextualisée* »[147].

[146] Dans sa décision n° 19-D-26 précitée, l'Autorité a en particulier enjoint Google à « *clarifier la rédaction des Règles Google Ads qui ont pour objet de protéger les utilisateurs de son moteur de recherche en ligne Google Search contre les annonces et les sites malveillants (ci-après : les « Règles Protectrices des Internautes »). À cet égard, la formulation des Règles Protectrices des Internautes doit comprendre non seulement leur définition, mais aussi leur nature en précisant le degré de gravité du manquement. La liste des Règles Protectrices des Internautes dont le manquement est considéré comme grave, et qui permet pour cette raison d'appliquer une procédure accélérée de suspension, doit être limitée à ce qui est strictement nécessaire et proportionné à l'objectif de protection du consommateur* ».

[147] Soulignement ajouté.

304. Sur cette disposition, certains acteurs du secteur entendus estiment que la communication d'informations relatives aux modalités de financement de l'application représente un gain de transparence pour l'utilisateur. Selon un acteur, l'utilisateur pourrait considérer cet élément comme un paramètre de choix entre les applications.

305. Cependant, certains acteurs du secteur précisent que le RGPD ne prévoit pas la communication de cette information aux utilisateurs et relèvent les difficultés de mise en œuvre d'une telle disposition dans la mesure où elle ne peut reposer que sur une déclaration des éditeurs dont la vérification serait très complexe, sinon impossible, pour les fournisseurs de magasins d'applications.

306. D'autre part, certains acteurs soulignent les risques concurrentiels qui résulteraient d'une obligation imposée aux éditeurs de fournir des informations détaillées sur le financement de leurs applications à des fins d'affichage par le magasin d'applications.

307. En premier lieu, les acteurs s'inquiètent de la nature et de la finesse des informations relatives aux modalités de financement susceptibles d'être collectées et affichées. À cet égard, ils relèvent l'imprécision de la disposition précitée. Par exemple, la mention relative à une « *réutilisation des données personnelles de l'utilisateur pour d'autres finalités* » recouvre, selon eux, de nombreux modes de financement possibles. Par ailleurs, certains soulignent que les informations visées ne devraient pas inclure d'informations détaillées révélant des informations sur la stratégie commerciale de l'éditeur (par exemple, l'identité des acquéreurs des données, des informations sur la tarification des données, la stratégie de vente de données spécifiques), dans la mesure où il s'agit d'informations sensibles sur le plan de la concurrence. Enfin, quand bien même l'affichage d'informations ne serait pas très détaillé, la disposition emporte le risque que les fournisseurs de magasins d'applications, également concurrents des éditeurs, collectent des données plus fines, et donc potentiellement sensibles, aux fins de réaliser cet affichage.

308. Sur ce point, l'Autorité relève l'ambiguïté de la disposition précitée dans la mesure où celle-ci fait simultanément référence à la pertinence de présenter l'information de façon synthétique à l'aide d'outils visuels et à la possibilité de contextualiser l'information. L'Autorité souligne en outre la nécessité de ne pas divulguer à des concurrents des informations sensibles sur le modèle de financement de l'application.

309. En second lieu, les acteurs interrogés s'inquiètent de la façon dont ces informations pourraient être présentées et en particulier, que cette présentation soit anxiogène pour l'utilisateur. Les acteurs ont ainsi souligné l'importance de contextualiser cette information. Ils soulignent les risques concurrentiels résultant d'une présentation imprécise ou erronée par les fournisseurs de magasins d'applications.

310. Par exemple, une mention sur la page de l'application indiquant « *cette application monétise vos données* » pourrait effectivement recouvrir différentes interprétations et effrayer les utilisateurs. Notamment, elle pourrait laisser penser que l'application revend les données des utilisateurs à des tiers, ce qui ne serait pas nécessairement le cas puisqu'il existe différentes façons de monétiser les données. Cette mention serait susceptible de distordre la concurrence si elle était imposée à des éditeurs qui fournissent ces données à des tiers pour une même finalité que des éditeurs traitant ces données en interne, par exemple dans un souci d'amélioration du ciblage publicitaire.

311. Certains acteurs considèrent important de rappeler que la réutilisation des données personnelles pour une finalité ultérieure n'est en outre pas interdite par le RGPD et clairement encadrée. En particulier, la réutilisation de données personnelles pour une finalité

différente est conditionnée au consentement de l'utilisateur. Le RGPD n'exige en revanche pas de justifier que les données vont engendrer un revenu.

312. Sur ce sujet, l'Autorité appelle à nouveau l'attention de la CNIL sur la nécessité, compte tenu du contexte concurrentiel décrit au paragraphe 257, de veiller à ce que les opérateurs verticalement intégrés ne puissent justifier la mise en œuvre de pratiques anticoncurrentielles par la mise en œuvre de ses recommandations.

313. À titre illustratif, tel pourrait être le cas si les fournisseurs de magasins d'applications souhaitaient désavantager les applications tierces concurrentes des leurs, en apposant sur les pages descriptives de ces applications une mention de nature à induire les consommateurs en erreur, en utilisant des termes pouvant être perçus comme dévalorisants ou en faisant une présentation partiale du mode de financement de ces applications.

Pour ces raisons, l'Autorité invite la CNIL à préciser sa disposition de façon à (i) ne pas encourager les fournisseurs de magasins d'applications à collecter des informations trop fines sur le financement des applications, en rappelant également l'interdiction, pour des « contrôleurs d'accès », d'utiliser les données des entreprises utilisatrices concurrentes (article 6(2) du DMA) ; (ii) ne pas afficher d'informations sur le modèle de financement des éditeurs qui iraient au-delà des obligations du RGPD ; et (iii) le cas échéant, prévoir la possibilité pour les éditeurs de renseigner manuellement et de manière personnalisée les informations destinées à un affichage, et en particulier de les contextualiser, ainsi que de renvoyer vers leur politique de confidentialité.

Sur la mise en œuvre de filtres dans l'interface de recherche ou d'un score relatifs à des critères de protection de la vie privée

314. À la section 9.3.1, les recommandations de la CNIL à l'égard des fournisseurs de magasins d'applications prévoient que :

« *Des filtres contenant des critères relatifs à la vie privée pourraient être directement mis à disposition dans l'interface de recherche. Ceux-ci pourraient être relatifs à l'utilisation de certaines permissions, la collecte de certaines données ou bien même relativement à un « score » relatif à des critères de vie privée.*

Si la création d'un tel score est envisagée, celui-ci devrait reposer sur une méthodologie préalablement définie et de manière transparente, de préférence par un acteur tiers au fournisseur de magasin d'applications et idéalement agréée entre les différents acteurs de l'écosystème et de la société civile. Le processus de calcul de ce score est susceptible d'être l'objet d'une certification, notamment pour assurer qu'il remplit ses objectifs en termes de transparence. Devraient également être mises à disposition les données sources permettant le calcul de ce score dans un format ouvert et facilement exploitable, afin que des méthodologies alternatives puissent être proposées.

Parmi les paramètres qui peuvent être pris en compte dans l'établissement de ce score peuvent figurer :

- *les types de données collectées (en fonction de leur sensibilité), leur volume et les finalités poursuivies,*
- *le nombre et le type de permissions demandées par l'application dès l'installation, ainsi que celles susceptibles de l'être au court de l'utilisation de l'application,*
- *le nombre et le type de SDK inclus dans l'application et les données qu'ils collectent en fonction des finalités,*

- *les mesures de sécurité mises en œuvre,*
- *la possibilité d'avoir accès au code source de l'application* ».

315. La section 9.3.2 prévoit en outre un mécanisme de signalement pouvant avoir un effet sur ce score :

« *Il devrait être permis aux utilisateurs de signaler les applications qui ne remplissent pas leurs obligations directement depuis le magasin d'applications, notamment en termes d'exercice des droits, de design trompeurs (« dark patterns ») de manquements aux consentements, d'exécution de fonctionnalités SDK sans consentement préalable, de présence de transferts non encadrés, etc.*

Ces remontées pourraient être utilisées pour orienter les contrôles sur les applications publiées et également impacter le score relatif aux critères de vie privées ».

316. Certains acteurs se montrent favorables à la mise en œuvre de filtres, voire d'un score, à condition que la mise en œuvre de ces dispositifs présente plusieurs garanties, en particulier la définition de critères précis, une évaluation des applications effectuée par la CNIL ou par un tiers indépendant, ainsi qu'un recueil d'informations préalables garantissant l'équité des éditeurs. Dans ce cas, de tels dispositifs pourraient apporter une meilleure transparence aux utilisateurs et leur permettre de mieux exercer leurs choix. D'un point de vue concurrentiel, ces dispositifs pourraient inciter les entreprises à se livrer concurrence en se fondant notamment sur le critère de la protection de la vie privée.

317. En revanche, la plupart des acteurs entendus se sont montrés opposés à cette disposition, dont la mise en œuvre par les fournisseurs de magasins d'applications serait en pratique difficile et pourrait être source de contestations, voire de contentieux, entre les parties impliquées.

318. En premier lieu, certains acteurs du secteur considèrent que la mise en œuvre de ces dispositions s'avérerait complexe si elle était confiée aux fournisseurs de magasins d'applications, étant donné l'impossibilité pour ces derniers d'accéder à certaines informations relatives aux traitements effectués sur les serveurs des développeurs et à la nécessité de réévaluer en continu le score de millions d'applications.

319. En deuxième lieu, de nombreux acteurs ont relevé l'absence de critères précis et objectifs tant pour l'élaboration des filtres que pour le calcul d'un score. Les critères mentionnés dans les recommandations de la CNIL dans le cadre de la liste non limitative citée ci-dessus ont fait l'objet de nombreuses critiques.

320. S'agissant du critère relatif au type de données, certains acteurs considèrent qu'il n'est pas pertinent à plusieurs égards. En effet, certaines applications collectant des données sensibles pour assurer leurs services aux utilisateurs, par exemple dans les domaines de la santé ou de la banque-assurance, pourraient être dotées d'un mauvais score. Plus généralement, des applications qui collectent beaucoup de données mais apportent beaucoup de valeur à l'utilisateur pourraient se trouver paradoxalement mal classées. Les acteurs soulignent en outre que les éditeurs collectant des données sensibles peuvent mettre en œuvre des mesures de sécurité fortes, tandis que des applications collectant moins de données ou des données moins sensibles pourront au contraire être sujettes à des vulnérabilités. Enfin, les applications dites « *freemium* » pourraient se trouver pénalisées relativement aux applications concurrentes reposant sur un modèle de financement payant, ce qui pourrait décourager les éditeurs à choisir ce modèle de financement et pénaliser les éditeurs dépendant de ce modèle. À cet égard, certains acteurs rappellent l'importance d'expliquer le

contexte et les finalités de toute collecte de données ainsi que la prévalence du consentement de l'utilisateur pour exercer ses choix.

321. S'agissant du critère relatif au nombre de permissions, un acteur interrogé a relevé que ce critère ne lui semblait pas révélateur de l'usage fait des données collectées.

322. S'agissant du critère relatif aux SDK, certains acteurs estiment que le nombre de SDK utilisés n'est pas nécessairement révélateur d'une moins bonne protection des données personnelles. De nombreux SDK ont en effet pu faire leurs preuves en matière de protection des données. Certains acteurs considèrent que ce critère est anxiogène à l'égard des SDK et donc défavorable à leur utilisation, alors que les SDK peuvent permettre de faciliter ou d'accélérer le développement de fonctionnalités logicielles.

323. Enfin, s'agissant du critère relatif aux signalements, certains acteurs considèrent que le score dépendrait alors d'un élément arbitraire, compte tenu d'une part de la nature hétérogène des plaintes et, d'autre part, de la latitude des fournisseurs de magasins d'applications de déterminer si la plainte est justifiée ou non, sans nécessairement avoir la connaissance du service ni du contexte des plaintes.

324. Plus généralement, la diversité des applications et les différentes manières dont elles fonctionnent rendraient difficile l'établissement de critères purement objectifs et neutres.

325. En dernier lieu, des acteurs du secteur relèvent que l'absence de critères et de méthodologie précis ainsi que de l'obligation de recourir à un tiers indépendant pour l'élaboration du score, pourrait conduire à l'élaboration de scores différents selon les magasins d'applications, ce qui irait à l'encontre de l'objectif affiché par la CNIL d'offrir aux utilisateurs un niveau suffisant d'information, leur permettant d'exercer leurs droits plus facilement.

326. Dans ce contexte, l'Autorité souligne que ces dispositifs de filtrage ou de score préconisés par la CNIL sont destinés à aider les utilisateurs à faire un choix éclairé. En revanche l'Autorité constate que le projet de la CNIL ne prévoit pas de liste de critères transparents, objectifs et non discriminatoires ni l'obligation de recourir à un acteur extérieur. Dans la mesure où les fournisseurs de magasins d'applications sont des acteurs verticalement intégrés dans la chaîne de valeur des applications mobiles, la mise en œuvre de ces dispositifs pourrait les placer dans la position d'être à la fois juge et partie. Ces derniers pourraient être tentés de modeler des dispositifs de filtrage ou de score de façon à servir leurs intérêts commerciaux et à fausser la concurrence.

327. À titre illustratif, sous prétexte de mesurer le score, les fournisseurs de magasins d'applications pourraient exiger que les éditeurs d'applications tierces concurrentes leur fournissent des informations non justifiées, leur permettant de détenir un avantage informationnel sur leurs concurrents.

328. Enfin, l'Autorité considère que le système de score envisagé par la CNIL n'établit pas clairement qu'un tel dispositif serait également applicable aux applications préinstallées, y compris les applications propriétaires des opérateurs verticalement intégrés. L'Autorité estime qu'il serait souhaitable que la CNIL précise ce point afin d'éviter tout risque de traitement différencié.

Sur ce sujet, à tout le moins, l'Autorité invite à la CNIL à préciser qu'un dispositif de score ne peut être conçu que par le régulateur ou par les pouvoirs publics, ou par un tiers indépendant sur la base de critères d'évaluation et d'exigences en matière de recueil d'informations qui soient proportionnés. Par ailleurs de tels dispositifs ne peuvent être mis en œuvre par des entreprises potentiellement en position dominante que de façon objective, transparente et non discriminatoire et ne peuvent être mis en œuvre par des plateformes qualifiées de contrôleurs d'accès que dans le respect des différentes dispositions du DMA, notamment les articles 6(2), 6(5)[148] et 6(12).

Il conviendrait enfin de rappeler que (i) la mise en œuvre d'un dispositif de score pourrait, afin d'assurer la fiabilité de cet indicateur, être sujet à un mécanisme de label ou de certification par un tiers indépendant ; et (ii) que si un magasin d'applications peut utilement proposer un mécanisme de signalements, il devrait communiquer les signalements reçus à la CNIL, autorité compétente pour juger de la conformité à la réglementation sur la protection des données personnelles pour le territoire français et le cas échéant, pour prononcer des sanctions.

Délibéré sur le rapport oral de Mme Corinne Aaron et Mme Martina Isola, rapporteures, Mme Mathilde Poulain, représentant le service économique et l'intervention de Mme Pascale Déchamps, rapporteure générale adjointe, par M. Thibaud Vergé, vice-président, président de séance, Mme Irène Luc et M. Henri Piffaut, vice-présidents.

La chargée de séance,	Le président de séance,
Claire Villeval	Thibaud Vergé

[148] L'article 6(5) du DMA fait notamment référence à l'interdiction d'auto-préférence du Gatekeepers dans les classements.