Réponse de l'AFNUM à la consultation publique de la Commission européenne sur le DMA

Introduction

L'AFNUM tient à saluer la proposition de Règlement relative aux marchés numériques (*Digital Market Act*, DMA), présentée le 15 décembre 2020 par la Commission Européenne. Ce texte **marque un développement important** en proposant de créer les conditions et le cadre réglementaire nécessaires à l'établissement d'un marché unique numérique plus fort et plus compétitif au sein de l'UE.

L'AFNUM tient à mettre en avant son attachement à une concurrence libre et loyale ainsi qu'au fait que les entreprises et les consommateurs européens puissent profiter des avantages du marché unique. Il convient de rappeler que les entreprises du secteur numérique ont stimulé l'innovation en Europe et développé l'emploi et la croissance, en fournissant des services à des centaines de milliers d'entreprises et à des millions de consommateurs. Elles jouent un rôle clé dans la mise en place d'un véritable marché unique numérique. Elles ont également permis de créer des opportunités d'expansion mondiale sans précédent permettant aux plus petits acteurs de se développer au-delà de leurs marchés d'origine.

Si l'AFNUM reconnaît l'intérêt que présente le DMA, **nous estimons toutefois que cette proposition de Règlement pourrait être améliorée à divers égards**, afin de mieux cibler les acteurs visés et de restreindre efficacement les pratiques commerciales ayant des conséquences lourdes sur l'équité du marché numérique.

I. Observations générales

Enjeux de l'approche horizontale du texte

La proposition de texte la Commission Européenne indique des critères de définition des « **contrôleurs d'accès** », acteurs soumis aux obligations du DMA.

Une entreprise est présumée remplir les critères la désignant comme un « contrôleur d'accès » si le fournisseur et le service de la plateforme dépassent certains seuils financiers et de base d'utilisateurs et répondent au critère « d'impact significatif », sachant que :

1) Un impact significatif sur le marché intérieur est présumé si le fournisseur a un chiffre d'affaires annuel dans l'EEE de plus de 6,5 milliards d'euros au cours des trois derniers exercices ou une capitalisation boursière moyenne de plus de 65 milliards d'euros au cours du dernier exercice ;

2) Un « service de plateforme essentiel » est présumé être une passerelle importante permettant aux « utilisateurs professionnels » d'atteindre les « utilisateurs finaux » si le « service de plateforme essentiel » compte plus de 45 millions d'utilisateurs actifs mensuels (MAU) dans l'UE et plus de 10 000 « utilisateurs professionnels actifs » annuels dans l'UE au cours du dernier exercice financier ;

3) Une position de marché bien établie et durable est présumée si les présomptions pour (1) et (2) ont été satisfaites au cours des trois dernières années.

Ces « contrôleurs d'accès » relèvent de nombreux modèles commerciaux différents qui ne se prêtent pas facilement à des règles horizontales. En effet, l'approche privilégiée consiste à appliquer un même

cadre et des mêmes obligations à un panel **d'acteurs connaissant des réalités très différentes**, dans le contexte de **marchés complexes et dynamiques**. **Imposer une pluralité de règles identiques** à un **panel d'entreprises très différentes** risque d'avoir des **conséquences indues** aussi bien sur les consommateurs que sur l'ensemble des acteurs du marché numérique.

Même si le DMA constitue avant tout une règlementation de marché, le consommateur ne figure pas dans la ligne directrice du texte. L'article 1.1 indique que « *Le présent règlement établit des règles harmonisées visant à garantir la contestabilité et l'équité des marchés dans le secteur numérique de l'Union là où des contrôleurs d'accès sont présents sur le marché* ». Cela nous interroge, notamment au regard du fait que l'intérêt du consommateur n'ait plus la même importance que dans la plupart des autres règlementations de l'UE.

Enfin, les activités et les services couverts par cette règlementation impliquent une approche qui tient compte de la réalité que connaissent certaines plateformes. Celles-ci, par leurs activités plurielles doivent équilibrer les intérêts de tous leurs utilisateurs (« utilisateurs finaux » et « utilisateurs professionnels ») et la viabilité du service dans son ensemble. Lorsque ces intérêts sont en conflit des décisions d'équilibrage difficiles sont nécessaires de la part des plateformes. **Cet élément ne transparait pas au sein de la proposition de texte.**

Cela montre que **le DMA ne semble pas prendre en compte l'ensemble des facteurs et privilégie une approche générale au regard du marché numérique.**

Une cohérence générale entre les textes européens est nécessaire

Par ailleurs, **il est impératif que le DMA soit en accord avec les autres textes européens déjà existants et futurs, pour assurer un cadre harmonisé pour l'ensemble des acteurs**.

Certains des services visés par la proposition de texte sont déjà couverts par d'autres textes. Par exemple, la proposition actuelle du Digital Services Act[1] (DSA), publiée parallèlement au DMA, vise à promouvoir une responsabilité accrue des fournisseurs de services d'hébergement, au vu de réduire la diffusion de contenus illégaux ou préjudiciables. Alors que le DSA oblige les plateformes à imposer des restrictions aux « utilisateurs professionnels », le DMA présente des exigences opposées. En effet, certaines obligations visent à empêcher le « contrôleur d'accès » d'avoir des leviers de contrôle sur les utilisateurs de sa plateforme (comme imposer des standards de cybersécurité), alors que le DSA veut augmenter la responsabilité des plateformes en traquant les utilisateurs frauduleux.

Le DMA et le DSA doivent être alignés, en particulier lorsqu'il s'agit de protéger les utilisateurs contre les dommages.

Il en va de même pour l'articulation avec le Règlement Général pour la Protection des Données[2] (RGPD). En l'espèce, comme nous le montrons plus bas, la proposition de règlementation nous paraît difficilement en phase avec le RGPD, s'agissant des obligations qui impliquent un traitement de données personnelles des utilisateurs des plateformes.

[1] RÈGLEMENT DU PARLEMENT EUROPÉEN ET DU CONSEIL relatif à un marché intérieur des services numériques (Législation sur les services numériques) et modifiant la directive2000/31/CE

[2] RÈGLEMENT (UE) 2016/679 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données).

II. Une proposition de texte dont l'équilibre reste à trouver

Les définitions et le champ d'application devraient être précisées

Certaines définitions manquent de lisibilité.

Pour garantir la sécurité juridique et la proportionnalité**, certaines définitions devraient être affinées ou alignées sur d'autres législations de l'UE.**

La définition « **d'utilisateurs professionnels actifs** » est très large : elle pourrait être interprétée comme incluant les revendeurs, les entrepreneurs principaux (utilisant un « contrôleur d'accès » comme sous-traitant) et les « utilisateurs professionnels » ayant recours aux services de la plateforme essentielle pour leurs fonctions internes. **Cette définition devrait se concentrer uniquement sur les utilisateurs ayant recours au « contrôleur d'accès » pour offrir ou promouvoir des services ou des biens.**

De même manière, la proposition de texte utilise le terme « **services de plateforme de base** » pour décrire un ensemble large et hétérogène de fournisseurs qui ont pour seule caractéristique commune l'utilisation d'une même technologie pour fournir leurs services. En effet, ces fournisseurs exploitent des modèles d'entreprise très divers, fournissent des services multiples, sont actifs sur des marchés distincts et monétisent leurs services de manière très différente. Par exemple, les obligations concernant la transparence des prix en matière de publicités et la validation des performances des publicités ne sont pas pertinentes pour les services qui ne sont pas monétisés par la publicité.

L'AFNUM s'interroge donc sur la pertinence **d'une définition regroupant des acteurs aussi hétérogènes**. D'autant plus que cette définition n'inclut finalement pas des acteurs tout aussi structurants du marché numérique, tels que les plateformes de streaming.

La notion de « **service de plateforme essentiel** » agissant comme une « **passerelle importante** » pour les utilisateurs professionnels vers les utilisateurs finaux en vertu de l'article 3(1)(b) doit également être clarifiée, afin que les services fournissant simplement un service technique et n'agissant pas comme intermédiaires ne soient pas désignés comme « contrôleur d'accès ».

A contrario, sans une définition plus précise, des services atteignant 10 000 « **utilisateurs professionnels** », qui eux-mêmes touchent 45 millions de clients pourraient entrer dans le champ d'application alors qu'il ne parait pas pertinent d'intégrer tous les services « cloud » dans le périmètre. Il ne serait notamment pas approprié d'inclure l'infrastructure en tant que service (IaaS) qui équivaut à du matériel virtuel et ne confère au fournisseur aucun rôle dans l'exploitation des services permettant à un utilisateur commercial d'atteindre ses « utilisateurs finaux ». De même, le cloud est fréquemment utilisé pour le stockage d'archives et n'agit pas comme un canal de commercialisation dans ce contexte.

Les « services d'informatique en nuage » doivent être exclus de la définition des « contrôleurs d'accès »

L'AFNUM s'interroge également sur les plateformes visées par la proposition de Règlement. En effet, cette dernière ne vise pas toutes les plateformes numériques. Elle se concentre sur les plates-formes qui servent « **d'intermédiaires directs** » entre les « utilisateurs professionnels » et les « utilisateurs finaux ».

Le texte indique que :

« *(…) on entend par (…) :*
2) « service de plateforme essentiel » : l'un des services suivants :
a) services d'intermédiation en ligne,
b) moteurs de recherche en ligne,
c) services de réseaux sociaux en ligne,
d) services de plateformes de partage de vidéos,
e) services de communications interpersonnelles non fondés sur la numérotation,
f) systèmes d'exploitation,
g) services d'informatique en nuage,
h) services de publicité, y compris tous réseaux publicitaires, échanges publicitaires et autre service d'intermédiation publicitaire, fournis par un fournisseur de l'un quelconque des services de plateforme essentiels énumérés aux points a) à g); »

Or, plusieurs « **services de plateforme de base** » ne présentent pas les caractéristiques du service ou les risques invoqués pour justifier le DMA. Par exemple, les services d'informatique en nuage sont utilisés directement par des clients pour accomplir des tâches et gérer des processus ou pour construire leurs propres solutions technologiques. **Ils ne servent pas, selon nous, d'intermédiaire dans la relation entre les « utilisateurs professionnels » et les « utilisateurs finaux » et ne répondent donc pas à la notion de « contrôleur d'accès ».**

Des modalités de désignation des « contrôleurs d'accès » questionnables

Comme indiqué ci-dessus, la proposition de texte de la Commission présente plusieurs critères de désignation des « contrôleurs d'accès ». Ces critères sont essentiellement **des critères quantitatifs,** qui apparaissent **questionnables,** au regard des **enjeux** que ce choix juridique soulève. Nous souhaitons montrer l'importance de prendre en compte les différents modèles économiques existants sur le marché numérique, et ainsi d'autres critères, pour désigner des « contrôleurs d'accès » qui le sont effectivement.

Il conviendrait, en effet, **de prendre en compte la réalité du nombre d'utilisateurs** (comme détaillé ci-dessous), **les parts de marché** (à défaut, certains moteurs de recherche subiraient les mêmes obligations que Google, bien qu'ils n'aient pas du tout la même place sur le marché) et **d'assurer la sécurité juridique des acteurs**.

Une désignation des « contrôleurs d'accès » qui ne tient pas compte des différents modèles existants sur le marché numérique

Le nombre d'utilisateurs actifs mensuels (MAU) et « d'utilisateurs professionnels » varie significativement d'une plateforme à une autre. Dès lors, il apparaît nécessaire de ne pas appliquer un critère de désignation uniforme pour l'ensemble des « contrôleurs d'accès ».

Par exemple, un utilisateur final peut créer un compte et utiliser plusieurs réseaux sociaux différents - soit Facebook, Instagram, Snapchat, Twitter, Reddit, TikTok, Pinterest et LinkedIn - ce qui fait augmenter le nombre d'utilisateurs de chacun de ces réseaux sociaux à partir d'un seul appareil. Cependant, un utilisateur ne peut utiliser qu'un seul système d'exploitation par appareil possédé. Par conséquent, le nombre d'utilisateurs actifs mensuels ne peut pas être mesuré de la même façon entre des acteurs où l'on peut facilement cumuler et créer des comptes, comme les réseaux sociaux, à l'inverse d'acteurs où le nombre de compte est très limité, comme pour les systèmes d'exploitation.

Dès lors, le seuil à partir duquel **le nombre d'utilisateurs actifs mensuels est indicatif de l'importance pourrait être différencié selon les catégories d'acteurs.**

Par ailleurs, le nombre d'utilisateurs actifs mensuels ne donne qu'une image partielle de l'importance d'un service financé par la publicité. En effet, même s'ils ont un nombre d'utilisateurs actifs mensuels élevé, **les services de plateforme financés par la publicité dont l'engagement et l'attention des utilisateurs finaux**, tels que certains réseaux sociaux, **sont faibles sont moins attrayants et moins pertinents** pour les annonceurs. **La proposition actuelle ne tient pas compte de ces distinctions**, et le texte pourrait s'appliquer à un large éventail de fournisseurs et de services de plateforme de base qui n'ont pas ou peu d'impact sur l'équité des marchés numériques.

Des critères de désignation représentatifs ?

Il convient de noter que les seuils spécifiques choisis par la Commission européenne ne sont pas toujours en mesure de démontrer une puissance de marché :

- **Les parts de marchés** ne sont pas prises en compte.
- L'obligation de fournir un « service de plateforme essentiel » dans **au moins 3 États membres** de l'UE soulève la question des entreprises qui remplissent les critères pour être définis « contrôleurs d'accès » mais ne fournissent pas leur service de plateformes dans a minima trois Etats membres.
- La taille importante d'une entreprise ne démontre pas nécessairement un manque de contestabilité sur le marché (c'est-à-dire qu'un « contrôleur d'accès » au niveau de l'UE n'est pas nécessairement un leader du marché dans chaque marché national).

La sécurité juridique des entreprises doit être assurée

Le processus de désignation des « contrôleurs d'accès » soulève des questionnements en matière de **sécurité juridique**, en particulier pour les entreprises proches du respect des seuils de présomption.

Le fait que la Commission européenne puisse utiliser des actes délégués pour développer et revoir la méthodologie de désignation risque de compromettre la sécurité juridique des entreprises en accordant à la Commission un pouvoir discrétionnaire trop important. En effet, dans la proposition de Règlement, des notions essentielles peuvent être modifiées en profondeur alors qu'elles peuvent avoir un impact sur le champ d'application du DMA. Par exemple, les critères de définition et de comptabilisation des « utilisateurs actifs » sont un élément très important s'agissant de la définition d'un « contrôleur d'accès ». Cela d'autant plus au regard de la pluralité de situations qui existent derrière ce terme et le fait que celui-ci renvoie aussi bien à des titulaires de comptes professionnels sur un service de marché en ligne qu'à des utilisateurs d'un service d'informatique en nuage.

Si **nous soutenons la nécessité d'une régulation européenne**[3] et le fait que **les pouvoirs accordés aux autorités nationales ne soient pas trop importants**, il convient cependant que des **mécanismes juridiques aussi importants** fassent **l'objet de procédures plus transparentes et de leviers plus contrôlés.**

[3] Comme demandé par M. le ministre Cédric O, Secrétaire d'Etat au numérique, à l'occasion d'un webinaire organisé par le Think-Tank CERRE « The DMA : EU, US and global perspectives » le 04/05/2021 :
« Il faut que le régulateur soit aussi européen que possible », « *comme nous le voyons dans le RGPD, des approches nationales différentes peuvent menacer le texte lui-même. La Commission ou une entité européenne doit pouvoir donner rapidement un arbitrage. Sans cela, le marché unique ne fonctionne pas* ».

D’autant plus que certains éléments manquent de clarté :

- Les trois principaux critères énoncés à l'article 3.1 (« Un impact significatif », une « porte d'entrée importante », une « position enracinée et durable ») même avec l'appui des critères quantifiables et qualitatifs, rendront difficile pour une entreprise ciblée de réfuter le processus de désignation.
- Les critères qualitatifs de l'article 3.6 ne garantissent pas que le régulateur prenne en considération les réalités du marché. Par exemple la notion de « autres caractéristiques du marché des structures » n'est pas définie et est trop large.

Un besoin de transparence accrue et d’une proportionnalité au service de la sécurité juridique

Enfin, il est essentiel de publier des lignes directrices sur la manière dont la Commission européenne évalue les critères de désignation des « contrôleurs d’accès ». Cela notamment du fait que la liste d’indicateurs proposés dans la proposition de texte et le concept de « contrôleurs d’accès » soient des concepts nouveaux dans le droit de l’UE. L’évaluation des mesures adoptées dans cette proposition de Règlement apparaît primordiale pour améliorer les règles en matière de marché numérique à l’avenir.

Dès lors, un principe de transparence se doit d’être assuré, **en imposant à la Commission de publier les décisions reflétant l’application des indicateurs** (à l’instar des dispositions prévues à l’article 7).

III. Des obligations sources de multiples effets de bords

L’un des enjeux majeurs de ce texte est de prévoir des obligations spécifiques aux acteurs désignés comme « contrôleurs d’accès ». C’est l’enjeu des articles 5 et 6 de la proposition de Règlement. L’AFNUM **reconnaît l’intérêt** que présentent ces obligations qui constituent, dans une large mesure, des outils au service de l’égalité des chances des acteurs du numérique et de la lutte contre les distorsions de concurrence.

Toutefois, la diversité des services, des modèles commerciaux et de l'intérêt pour l'économie des plates-formes **rend une approche universelle difficile pour garantir la proportionnalité et des résultats bénéfiques**.

Le fait d’appliquer de mêmes obligations à un ensemble d’acteurs hétérogènes risque de réglementer des pratiques qui ne sont généralement pas préoccupantes et de créer des effets secondaires indésirables pour les modèles commerciaux pour lesquels ils n'ont pas été conçus à l'origine.

Par exemple, les obligations relatives à l’ouverture des données (article 6.1.i, détaillé ci-dessous) risquent d’affaiblir le niveau de sécurité des données détenues collectées par le « contrôleur d’accès ». Une fois les données partagées ou rendues accessibles, son propriétaire d’origine n’a plus de contrôle et ne peut assurer la sécurité de celles-ci. Dans ce cas, il conviendrait de ne pas imposer l’ouverture de l’ensemble des données à l’ensemble des acteurs, pour éviter des enjeux de sécurité trop important.

Dès lors, indépendamment des pratiques commerciales déloyales très clairement définies, **l’AFNUM recommande une approche avec des obligations adaptées selon les catégories d’acteurs.**

À ce titre, la Commission pourrait être autorisée, sur demande motivée du « contrôleur d'accès », à suspendre exceptionnellement, en tout ou partie, une obligation spécifique lorsque son application n'est pas injuste à l'égard des « utilisateurs professionnels » du service et ne porte manifestement pas atteinte aux principes de concurrence.

Afin d'illustrer la nécessité de prendre en compte la pluralité d'acteurs s'agissant des obligations, nous nous permettons de commenter ci-dessous plusieurs obligations qui présentent des enjeux différenciés selon les acteurs.

Le DMA risque de générer plusieurs « passagers clandestins » économiques

L'article 5 (c) indique que le « contrôleur d'accès » « *permet aux entreprises utilisatrices de promouvoir leurs offres auprès des utilisateurs finaux acquis grâce au service de plateforme essentiel, et de conclure des contrats avec ces utilisateurs finaux, en utilisant ou non à cette fin les services de plateforme essentiels du contrôleur d'accès, et permet aux utilisateurs finaux, par l'intermédiaire des services de plateforme essentiels du contrôleur d'accès, d'accéder à des contenus, abonnements, fonctionnalités ou autres éléments et de les utiliser en se servant de l'application logicielle de l'entreprise utilisatrice, lorsque ces éléments ont été acquis par les utilisateurs finaux auprès des entreprises utilisatrices concernées sans avoir recours aux services de plateforme essentiels du contrôleur d'accès;* »

Cette rédaction présente un risque de **« passager clandestin »** ou de rendre impossible, à grande échelle, l'applicabilité **des modèles commerciaux basés sur les commissions**. Par exemple, cela pourrait transformer les magasins d'applications en plateformes publicitaires non rémunérées - permettant aux vendeurs d'attirer les utilisateurs et de les diriger ensuite vers l'achat sur leurs propres sites.

Afin d'éviter cette problématique, un fournisseur de « services de plateforme essentiel » se doit d'avoir **des moyens de contrôle** sur ses « utilisateurs professionnels » **pour prévenir les abus** de son modèle de distribution.

Les exigences d'interopérabilité ne doivent pas porter atteinte à la sécurité et à la protection des données

L'article 6.1.c indique que le « contrôleur d'accès » « *permet l'installation et l'utilisation effective d'applications logicielles ou de boutiques d'applications logicielles de tiers utilisant, ou interopérant avec, les systèmes d'exploitation du contrôleur d'accès, et permet l'accès à ces applications logicielles ou boutiques d'applications logicielles par des moyens autres que les services de plateforme essentiels du contrôleur d'accès. Rien n'empêche le contrôleur d'accès de prendre des mesures proportionnées dans le but d'éviter que les applications logicielles ou les boutiques d'applications logicielles de tiers ne compromettent l'intégrité du matériel informatique ou du système d'exploitation qu'il fournit ;* »

L'article 6.1.f lui dispose que le « contrôleur d'accès » « *permet aux entreprises utilisatrices et aux fournisseurs de services accessoires d'accéder aux mêmes fonctionnalités du système d'exploitation, du matériel informatique ou du logiciel que celles qui sont disponibles ou utilisées dans le cadre de la fourniture de tout service accessoire par le contrôleur d'accès, et d'interopérer avec ces fonctionnalités ;* ».

Ces deux articles et les clauses d'interopérabilités qu'ils impliquent présentent de forts enjeux **en matière de cybersécurité et de protection des données.**

Les systèmes d'exploitation sont des plateformes techniques qui gèrent le matériel et les interfaces utilisateur et sont au cœur du fonctionnement des appareils. Ils jouent un rôle clé dans la gestion des performances des appareils et garantissent le respect des règles de sécurité des produits. Ceci est particulièrement important dans un contexte où les terminaux se multiplient (mobile, portable et IoT) et où l'appareil héberge et génère des quantités importantes de données personnelles.

Dès lors, **les éléments imposés aux articles 6.1.c et 6.1.f peuvent engendrer de nombreuses failles en matière de cybersécurité, de confidentialité** et représentent un défi technique de compatibilité important (entre Windows et IOS par exemple). En effet, fournir un accès tiers à une fonctionnalité technique spécifique a des implications importantes pour l'utilisateur.

Du point de vue du consommateur, l'accès peut avoir un impact sur l'expérience utilisateur et la sécurité (en ayant des difficultés à assurer le niveau de conformité nécessaire du fait de l'incompatibilité), affectant ainsi la confiance des utilisateurs pour la technologie ou le service sous-jacent. S'agissant des « utilisateurs professionnels », ils doivent pouvoir compter sur un accès à des fonctionnalités stables et matures de la part de la plateforme pour pouvoir investir, innover et, dans certains cas, créer une entreprise et des moyens de subsistance.

De même manière, une **interopérabilité obligatoire** doit être **très clairement définie** pour éviter des conséquences involontaires sur la sécurité, la confidentialité et la sûreté des utilisateurs et pour garantir l'innovation. **Il nous apparaît donc important d'être plus prudent, s'agissant des clauses générales d'interopérabilité dans le DMA**.

Des problématiques similaires sont posées par l'article 6.1.i et les données des « utilisateurs professionnels ». Celui-ci demande au « contrôleur d'accès » de procurer *« gratuitement aux entreprises utilisatrices, ou aux tiers autorisés par les entreprises utilisatrices, un accès et une utilisation effectifs, de haute qualité, continus et en temps réel pour les données agrégées ou non agrégées fournies ou générées dans le cadre de l'utilisation des services de plateforme essentiels concernés par ces entreprises utilisatrices et par les utilisateurs finaux qui se servent des produits et services qu'elles fournissent; en ce qui concerne les données à caractère personnel, ne procure l'accès et l'utilisation que lorsqu'ils sont directement liés à l'utilisation faite par l'utilisateur final en lien avec les produits ou services que l'entreprise utilisatrice concernée fournit par l'intermédiaire du service de plateforme essentiel concerné, et lorsque l'utilisateur final opte pour un tel partage de données en manifestant son consentement au sens du règlement (UE) 2016/679;* ».

Dans l'état actuel de sa rédaction, cet article pourrait forcer les fournisseurs de services qui ne collectent que des données client sur une base anonyme à réidentifier l'utilisateur afin de se conformer aux exigences d'accès aux données non agrégées des utilisateurs professionnels**. Ce point présente en plus des enjeux de conformité au RGPD et des contraintes techniques relatives au transfert de données difficiles à mettre en œuvre.**

Pré-installation

Enfin, en ce qui concerne la désinstallation d'applications préinstallées, soit l'article 6.1.b qui impose que le « contrôleur d'accès » « *permet aux utilisateurs finaux de désinstaller toute application logicielle préinstallée dans son service de plateforme essentiel, sans préjudice de la possibilité pour le contrôleur d'accès de restreindre cette désinstallation si elle concerne une application logicielle essentielle au fonctionnement du système d'exploitation ou de l'appareil et qui ne peut techniquement pas être proposée séparément par des tiers;* »**.**

Cette pratique est déjà adoptée par de nombreux fournisseurs de services. De plus, certaines applications préinstallées sont essentielles au fonctionnement d'un appareil, tout au long de son cycle de vie, pour contrôler des interfaces et des outils matériels ou bien pour accéder à d'autres services et contenus (comme les magasins d'applications et les navigateurs par exemple). En outre, les consommateurs s'attendent à une expérience prête à l'emploi lors de l'achat d'un appareil.

Ainsi, la référence de l'article 6.1.b aux services **qui « ne peuvent pas être techniquement proposés de manière autonome par des tiers » est trop restrictive** pour garantir une expérience utilisateur adéquate **tout au long du cycle de vie de l'appareil**.

IV. Observations finales

Dialogue règlementaire

Le dialogue réglementaire est décrit comme important dans le considérant 33 : « *Il est nécessaire en outre de prévoir la possibilité d'établir, avec les contrôleurs d'accès, un dialogue sur les mesures de régulation à prendre, pour adapter ces obligations susceptibles de requérir des mesures de mise en œuvre spécifiques afin de garantir leur efficacité et leur proportionnalité.* ». Nous soutenons cette idée de dialogue dans le souci d'une application efficace et d'une meilleure mise en œuvre des obligations (articles 5 et 6).

Cependant, ce dernier est encadré essentiellement par les pouvoirs d'enquête du régulateur, sous la menace de sanctions importantes. Il n'est également mentionné qu'au sein d'un nombre limité d'articles, tel que l'article 7 dans le cadre de l'attribution des obligations où « *la Commission fait part de ses constatations préliminaires dans un délai de trois mois à compter de l'ouverture de la procédure. Dans ses constatations préliminaires, la Commission explique les mesures qu'elle envisage de prendre ou que le fournisseur de services de plateforme essentiels concerné devrait prendre, selon elle, afin de donner suite de manière effective aux constatations préliminaires*. ».

Il nous apparaît essentiel que les différentes parties aient **la possibilité d'engager un dialogue en dehors des pouvoirs d'enquête et d'attribution du régulateur**. Ce dialogue devrait également avoir lieu dans le contexte d'un ensemble plus large d'articles du DMA, tels que l'article 3 sur le processus de désignation ou l'article 17 - qui permet au régulateur de revoir la liste des services et obligations de base de la plateforme.

Dans le cadre de ce dialogue, les parties concernées pourront expliquer des comportements spécifiques sur la base d'avis motivés, à la lumière des objectifs du DMA et dans le respect d'autres textes réglementaires. Un tel dialogue permettrait une adaptation des obligations aux réalités propres à chaque acteur et ainsi une règlementation plus adéquate au marché numérique.

Cela mènera finalement à des décisions plus ciblées et plus rapides, fondées sur des preuves et limitant la possibilité de conséquences involontaires. Cela réduira également la perspective d'appels devant les tribunaux, ce qui retarderait davantage l'impact positif du DMA sur le marché. Ce dialogue doit être mené sans incidences sur la capacité du régulateur à lancer des enquêtes formelles.

Dans cette optique, nous saluons les mesures de concertations prévues par la Commission qui permettent aux acteurs de réfuter la désignation de « contrôleur d'accès » sur la base de critères quantifiables afin d'examiner également des critères qualitatifs.

A propos de l'AFNUM

L'AFNUM (Alliance Française des Industries du Numérique) représente, en France, les industriels du secteur IT, des réseaux, de l'électronique grand public, de l'impression, de la photographie et des objets connectés. Le poids économique des 56 entreprises adhérentes de l'AFNUM est de 31.000 emplois directs et de 60.000 emplois indirects et induits en France pour 26 milliards d'euros de chiffre d'affaires. L'AFNUM est membre de la FIEEC, du MEDEF et de Digitaleurope.

(Airbus DS, Alcad, Alcatel Lucent Enterprise, Amazon, Apple, Art-Fi, Brother, Cae, Canon, Cisco, Continental, Crosscall, Dell, Doc up, Epson, Erard, Ericsson, FP Francotyp-Postalia, Fracarro, Fujifilm, HP, IBM, Intel, Kodak alaris, Leica, Lenovo, Lexmark, LG, Lumiere Imaging, Microsoft, Nikon, Nokia, Oppo, Optex Normand, Panasonic, Quadient (ex-Neopost), Qwant, Ricoh imaging, Samsung, Sequans Communications, Sigma, Sony, Storit.io, Tamron, TCL, Technicolor, Televes, Tetenal, Toshiba, Trax, Triax, Verbatim, Vitec Imaging Distribution, WDC, WISI)