Règlement sur les services numériques (DSA) et marchés numériques (DMA)

L'Union européenne (UE) a mis en place une nouvelle législation, inédite au plan mondial, pour réguler Internet et ses risques

- **le règlement sur les marchés numériques** dit **DMA** (pour *Digital Markets Act*), qui entend prévenir les abus de position dominante des géants du numérique, que sont en particulier les GAFAM (*Google*, *Apple*, *Facebook*, *Amazon* et *Microsoft*), et offrir un plus grand choix aux consommateurs européens ;
- **le règlement sur les services numériques** dit **DSA** (pour *Digital Services Act*), qui prévoit de lutter contre les contenus et produits illégaux en ligne (haine, désinformation, contrefaçons...). L'objectif est de faire d'internet un espace plus sûr pour les utilisateurs. Avec ce texte, "*ce qui est illégal dans le monde physique le sera aussi en ligne*".

1 – Règlement européen DSA

Le règlement DSA (pour *Digital Services Act)* du 19 octobre 2022 est, avec le règlement sur les marchés numériques (DMA), un des grands chantiers numériques de l'Union européenne (UE).

Les obligations prévues par ce texte doivent entrer en application le 17 février 2024. Les très grandes plateformes en ligne et les très grands moteurs de recherche sont concernés plus tôt, dès le 25 août 2023.

1 – 1 – objectifs du DSA

La législation sur les services numériques (DSA) veut mettre en pratique le principe selon lequel **ce qui est illégal hors ligne est illégal en ligne.**

Elle fixe un ensemble de règles pour responsabiliser les plateformes numériques et lutter contre la diffusion de contenus illicites ou préjudiciables ou de produits illégaux : attaques racistes, images pédopornographiques, désinformation, vente de drogues ou de contrefaçons... Cette législation succède à la directive dite e-commerce du 8 juin 2000, devenue dépassée.

Les objectifs sont multiples :

- mieux protéger les internautes européens et leurs droits fondamentaux (liberté d'expression, protection des consommateurs...) ;
- aider les petites entreprises de l'UE à se développer ;

- renforcer le contrôle démocratique et la surveillance des très grandes plateformes et atténuer leurs risques systémiques (manipulation de l'information...)

1 – 2 - Quels sont les acteurs visés par le DSA ?

Le règlement DSA doit s'appliquer à tous les intermédiaires en ligne qui offrent leurs services (biens, contenus ou services) sur le marché européen. Peu importe que ces intermédiaires soient établis en Europe ou ailleurs dans le monde.

Sont notamment concernés :

- Les fournisseurs d'accès à internet (**FAI**) ;
- Les services d'informatique en nuage (***cloud***) ;
- Les plateformes en ligne comme les places de marché **(*market places***), les boutiques d'applications, les réseaux sociaux, les plateformes de partage de contenus, les plateformes de voyage et d'hébergement ;
- **les très grandes plateformes en ligne (VLOP** - Very large Online Platforms**) et les très grands moteurs de recherche (VLOSE –** Very Large Online Search Engines) , utilisés par plus de 45 millions d'Européens par mois, désignés par la Commission européenne.

Le 25 avril 2023, une première série de ces grands acteurs en ligne a été publiée sur le site de la Commission. Sont visées 17 très grandes plateformes :

Très grandes plateformes en ligne : VLOP

- Alibaba AliExpress
- Boutique Amazon
- AppStore d'Apple
- Booking.com
- Facebook (en anglais)
- Google Play
- Google Maps
- Google Shopping
- Instagram (en anglais)
- LinkedIn (en anglais)
- Pinterest (en anglais)
- Snapchat (en anglais)
- TikTok
- Twitter

- Wikipédia
- YouTube
- Zalando

Très grands moteurs de recherche en ligne : VLOSE

- Terril
- Recherche Google

Les plateformes ont été désignées sur la base des données des utilisateurs qu'elles devaient publier avant le 17 février 2023.

Toutes ces entreprises doivent se conformer au DSA au 25 août 2023.

1 – 3 - Que va changer le DSA ?

Le *Digital Services Act* prévoit de nombreuses mesures, graduées selon les acteurs en ligne en fonction de la nature de leurs services et de leur taille. Les très grandes plateformes et les très grands moteurs de recherche sont soumis à des exigences plus strictes. Tous les acteurs en ligne vont devoir désigner un point de contact unique ou, s'ils sont établis hors UE, un représentant légal et coopérer avec les autorités nationales en cas d'injonction. Les autres obligations peuvent être classées en trois catégories.

1-3- 1- Lutte contre les contenus illicites

Les plateformes en ligne doivent proposer aux internautes un outil leur permettant de signaler facilement les contenus illicites. Une fois le signalement effectué, elles doivent rapidement retirer ou bloquer l'accès au contenu illégal. Dans ce cadre, elles coopèrent avec des "signaleurs de confiance". Ce statut est attribué dans chaque pays à des entités ou organisations en raison de leur expertise et de leurs compétences. Leurs notifications sont traitées en priorité.

Les ***market places*** (tels Aibnb ou Amazon) doivent mieux tracer les vendeurs qui proposent des produits ou services sur leur plateforme (recueil d'informations précises sur le professionnel avant de l'autoriser à vendre, vérification de la fiabilité de celles-ci) et mieux en informer les consommateurs.

1 – 3 – 2 - Transparence en ligne

Les plateformes doivent rendre plus transparentes leurs décisions en matière de modération des contenus. Elles doivent prévoir un système interne de traitement des réclamations permettant aux utilisateurs dont le compte a été suspendu ou résilié (par exemple sur un réseau social) de contester cette décision. Pour régler le litige, les

utilisateurs peuvent également se tourner vers des organismes indépendants et certifiés dans les pays européens ou saisir leurs juges nationaux.

Les plateformes doivent par ailleurs expliquer le fonctionnement des algorithmes qu'elles utilisent pour recommander certains contenus publicitaires en fonction du profil des utilisateurs. Les très grandes plateformes et les très grands moteurs de recherche doivent proposer un système de recommandation de contenus non-fondé sur le profilage et mettre à disposition du public un registre des publicités contenant diverses informations (qui a parrainé l'annonce, comment et pourquoi elle cible tels individus...).

La publicité ciblée pour les mineurs devient interdite pour toutes les plateformes, de même que la publicité basée sur des données sensibles comme les opinions politiques, la religion ou l'orientation sexuelle (sauf consentement explicite).

Les interfaces trompeuses connues sous le nom de "pièges à utilisateurs" (*dark patterns*) et les pratiques visant à induire les utilisateurs en erreur (mise en avant de certains choix...) sont prohibées.

1 – 3 – 4 - Atténuation des risques et réponse aux crises

Les très grandes plateformes et les très grands moteurs de recherche jouent un rôle très important et influent sur la sécurité en ligne, la diffusion de l'information, la formation de l'opinion publique et les transactions économiques. C'est pourquoi d'autres mesures leurs sont imposées, proportionnées aux risques sociétaux qu'ils représentent lorsqu'ils diffusent des contenus illicites ou préjudiciables, comme la désinformation. Ces grands acteurs doivent désormais :

- Analyser tous les ans les risques systémiques qu'ils génèrent (sur la haine et la violence en ligne, les droits fondamentaux, le discours civique, les processus électoraux, la santé publique...) et prendre les mesures nécessaires pour atténuer ces risques (respect de codes de conduite, suppression des faux comptes, visibilité accrue des sources d'information faisant autorité...) ;
- Effectuer tous les ans des audits indépendants de réduction des risques, sous le contrôle de la Commission européenne ;
- Fournir les algorithmes de leurs interfaces à la Commission et aux autorités nationales compétentes ;
- Accorder un accès aux données clés de leurs interfaces aux chercheurs pour qu'ils puissent mieux comprendre l'évolution des risques en ligne ;
- Mieux protéger les mineurs en ligne.

Un **mécanisme de réaction aux crises touchant la sécurité ou la santé publique** est enfin prévu. La Commission européenne va pouvoir demander aux grands acteurs une analyse des risques que posent leurs interfaces lorsqu'une crise émerge (comme lors de

l'agression russe contre l'Ukraine) et leur imposer pendant un temps limité des mesures d'urgence.

1 – 3 – 5 - Quelle surveillance et quelles sanctions en cas de non-respect du DSA ?

Dans tous les pays de l'UE, un "coordinateur des services numériques", autorité indépendante désignée par chaque État membre, est mis en place. En France, le coordinateur national sera l'Arcom, tel que le prévoit le projet de loi visant à sécuriser et réguler l'espace numérique. Dans d'autres pays, il s'agira aussi de l'autorité des médias.

Ces 27 coordinateurs vont être chargés de contrôler le respect du règlement DSA dans leur pays et de recevoir les plaintes à l'encontre des intermédiaires en ligne. Ils coopéreront au sein d'un "comité européen des services numériques" qui rendra des analyses, mènera des enquêtes conjointes dans plusieurs pays et émettra des recommandations sur l'application de la nouvelle réglementation. Ce comité devra notamment recommander la Commission sur l'activation du mécanisme de réponse aux crises.

Les très grandes plateformes en ligne et les très grands moteurs de recherche vont être surveillés par la Commission européenne. Pour financer cette surveillance, des "frais de supervision" leur sont demandés, dans la limite de 0,05% de leur chiffre d'affaires annuel mondial.

En cas de non-respect du DSA, des astreintes et des sanctions pourront être prononcées. Pour les très grandes plateformes et les très grands moteurs de recherche, la Commission pourra infliger des amendes pouvant aller jusqu'à 6% de leur chiffre d'affaires mondial.

En cas de violations graves et répétées au règlement, les plateformes pourront se voir interdire leurs activités sur le marché européen.

2 – Règlement Européen DMA

Les géants du Net vont bientôt devoir respecter de nouvelles obligations et interdictions sous peine de lourdes amendes, en vertu du règlement sur les marchés numériques (DMA). L'Union européenne veut mettre fin à la domination de ces géants en leur imposant des règles qui profiteront aux entreprises et aux internautes européens.

2 – 1 - Quels sont les objectifs du règlement DMA ?

La législation sur les marchés numériques (DMA) vise à **lutter contre les pratiques anticoncurrentielles des géants d'internet** et **corriger les déséquilibres de leur domination** sur le marché numérique européen.

Le modèle économique de ces acteurs, **en particulier des GAFAM (Google, Apple, Facebook, Amazon et Microsoft),** repose sur la combinaison de masses de données sur leurs utilisateurs et d'algorithmes puissants et opaques. Grâce aux forts effets de réseau et à leurs écosystèmes enfermant les internautes-consommateurs, ces grands acteurs ont acquis une **position de quasi-monopole sur le marché européen**, laissant peu de place à la concurrence. À eux seuls, les GAFAM représentent un chiffre d'affaires comparable aux recettes fiscales de la France.

Selon la Commission européenne, plus de 10 000 plateformes en ligne – dont 90% sont des petites et moyennes entreprises - opèrent en Europe, mais seules les plus grandes plateformes dites "systémiques" captent l'essentiel de la valeur du marché numérique européen.

C'est pourquoi des **outils de régulation sont mis en place en amont** pour :

- **Créer** une concurrence loyale entre les acteurs du numérique, notamment au profit des petites et moyennes entreprises et des *start-up* européennes ;
- **Stimuler** l'innovation, la croissance et la compétitivité sur le marché numérique ;
- **Renforcer** la liberté de choix des consommateurs européens.

Cette régulation *a priori (ex ante*) vient compléter le droit de la concurrence. Le droit de la concurrence, qui sanctionne *a posteriori (ex post*) des ententes ou des abus de position dominante, ne suffit plus aujourd'hui à réguler efficacement le marché numérique. Les amendes prononcées par la Commission européenne ou par les autorités nationales de la concurrence interviennent en effet souvent trop tard, après de longues enquêtes. Cette lenteur des procédures n'incite pas les géants d'internet à modifier en profondeur leur comportement, sans compter les recours judiciaires qui suivent.

Avec cette nouvelle législation, l'UE veut devenir un modèle, au niveau mondial, dans le domaine de l'économie numérique.

2 – 2 - Quelles sont les activités visées par le DMA ?

Le règlement couvre des services en ligne très répandus et couramment utilisés, fournis ou proposés par les grandes plateformes. Il liste **dix "services de plateforme essentiels" ou de base** qui posent aujourd'hui problème. Il s'agit des :

- Services d'intermédiation (comme les places de marché, les boutiques d'applications) ;
- Moteurs de recherche ;
- Réseaux sociaux ;
- Plateformes de partage de vidéos ;
- Messageries en ligne ;

- Systèmes d’exploitation (dont les télévisions connectées) ;
- Services en nuage (*cloud*) ;
- Services publicitaires (tels les réseaux ou les échanges publicitaires) ;
- Navigateurs web ;
- Assistants virtuels**.**

2 – 3 - Quelles sont les entreprises concernées par le DMA ?

Le règlement DMA cible uniquement les entreprises qui sont des "contrôleurs d’accès" à l'entrée d'internet, les gardes-barrières *(gatekeepers*) de l'internet. Il s’agit d’acteurs qui ont une forte incidence sur le marché intérieur, sont un point d’accès important des entreprises utilisatrices pour toucher leur clientèle et occupent ou occuperont dans un avenir proche une position solide et durable. Peu importe qu’ils soient établis en Europe ou ailleurs dans le monde.

Sont présumées être des contrôleurs d’accès, au sens de la nouvelle législation européenne, les entreprises qui :

- Fournissent un ou plusieurs services de plateforme essentiels dans au moins trois pays européens ;
- Ont un chiffre d’affaires ou une valorisation boursière très élevé : 7,5 milliards d'euros au moins de chiffre d'affaires annuel en Europe dans les trois dernières années ou 75 milliards d'euros ou plus de capitalisation boursière durant la dernière année ;
- Enregistrent un grand nombre d’utilisateurs dans l'UE : plus de 45 millions d'Européens par mois et 10 000 professionnels par an pendant les trois dernières années.

Les entreprises qui atteignent ces seuils chiffrés avaient jusqu'au 3 juillet 2023 pour s’identifier. Le 6 septembre 2023, la Commission européenne a publié une première liste de six contrôleurs d'accès.

La Commission a ouvert, par ailleurs, quatre enquêtes de marché, afin d'examiner d'ici cinq mois les observations de Microsoft et d'Apple qui font valoir que Bing, Edge, Microsoft Advertising et iMessage ne peuvent être considérés comme des points d'accès au sens du DMA. Une autre enquête de marché est en cours concernant l'iPadOS d'Apple, qui bien que n'atteignant pas le seuils fixés par la législation, pourrait être désigné comme contrôleur d'accès.

Les entreprises concernées peuvent contester leur désignation.

La liste des contrôleurs d'accès et la liste des services de plateforme essentiels qu'ils fournissent seront révisées au moins tous les trois ans.

À savoir : les PME sont - hors cas exceptionnels - exemptées de la qualification de contrôleur d'accès. Une catégorie de "contrôleur d'accès émergent" est également prévue, afin d'imposer certaines obligations aux entreprises dont la position concurrentielle est démontrée mais pas encore durable.

2 – 4 - Que va changer le DMA ?

. Les entreprises désignées comme *gatekeepers* devront nommer un ou plusieurs responsables de la conformité avec le règlement, sous peine d'amende, et respecter **d'ici le 6 mars 2024 une petite vingtaine d'obligations ou d'interdictions**, pour chacun de leurs services de plateforme essentiels. Certaines sont applicables à tous, d'autres seront prononcées sur mesure.

Les contrôleurs d'accès devront par exemple :

- Rendre aussi facile le désabonnement que l'abonnement à un service de plateforme essentiel ;
- Permettre de désinstaller facilement sur son téléphone, son ordinateur ou sa tablette des applications préinstallées ;
- Rendre interopérables les fonctionnalités de base de leurs services de messagerie instantanée (Whatsapp, Facebook Messenger…) avec leurs concurrents plus modestes ;
- Autoriser les vendeurs à promouvoir leurs offres et à conclure des contrats avec leurs clients en dehors des plateformes ;
- Donner aux vendeurs l'accès à leurs données de performance marketing ou publicitaire sur leur plateforme ;
- Informer la Commission européenne des acquisitions et fusions qu'ils réalisent.

Les contrôleurs d'accès ne pourront plus notamment :

- Imposer les logiciels les plus importants (navigateur web, moteurs de recherche, assistants virtuels) par défaut à l'installation de leur système d'exploitation. Un écran multi-choix devra être proposé pour pouvoir opter pour un service concurrent ;
- Favoriser leurs services et produits par rapport à ceux des vendeurs qui utilisent leur plateforme (auto-préférence) ou exploiter les données des vendeurs pour les concurrencer ;
- Réutiliser les données personnelles d'un utilisateur à des fins de publicité ciblée, sans son consentement explicite ;
- Imposer aux développeurs d'application certains services annexes (système de paiement par exemple).

Une personne lésée par un contrôleur d'accès pourra s'appuyer sur la liste de ces obligations et interdictions pour demander des dommages et intérêts devant les juges nationaux.

2 – 5 - Quelles sanctions en cas de non-respect du DMA ?

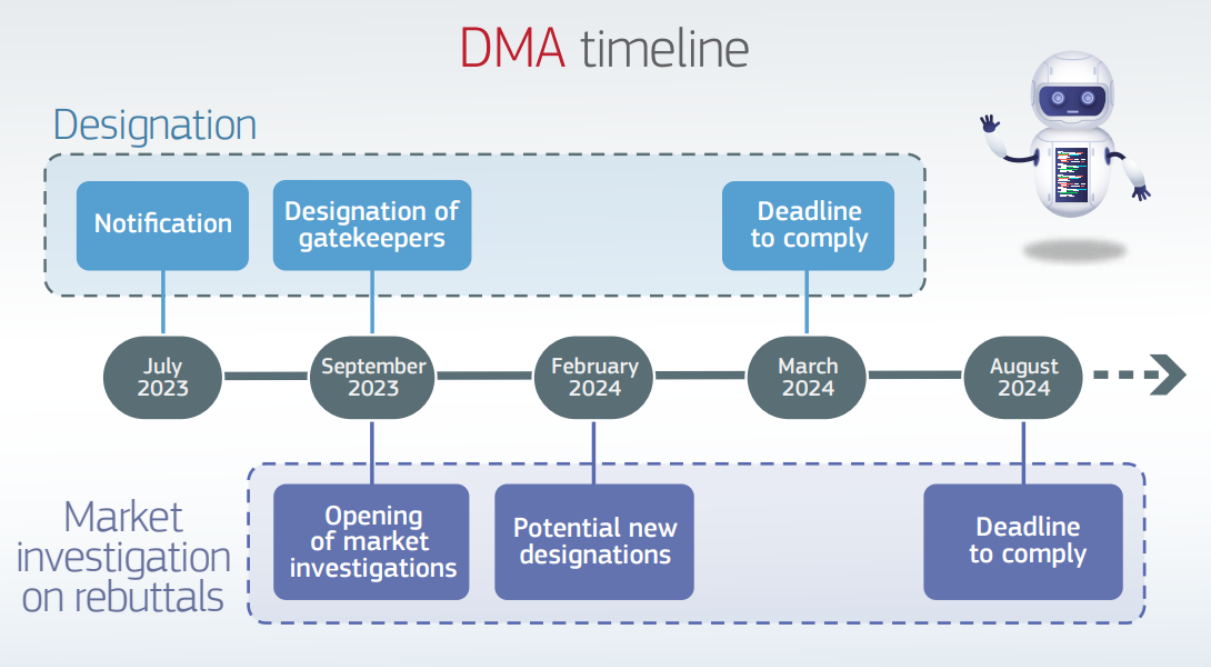
En cas d'infraction, la Commission européenne pourra prononcer contre le contrôleur d'accès une **amende pouvant aller jusqu'à 10% de son chiffre d'affaires mondial total** et, **en cas de récidive, jusqu'à 20%** de ce chiffre d'affaires. Elle pourra aussi prononcer des astreintes allant jusqu'à 5% de son chiffre d'affaires journalier mondial total.

Si l'entreprise viole systématiquement la législation européenne, à savoir à partir de "trois violations sur huit ans", la Commission pourra ouvrir une enquête de marché et, si besoin, imposer des mesures correctives comportementales ou structurelles. La Commission européenne pourra, par exemple, **obliger le contrôleur d'accès à céder une activité** (vente d'unités, d'actifs, de droits de propriété intellectuelle ou de

marques) **ou lui interdire d'acquérir des entreprises** de services dans le numérique ou de collecte de données.

À noter : Les autorités nationales de la concurrence pourront enquêter sur d'éventuelles infractions aux règles du DMA et transmettre leurs conclusions à la Commission.

Le Planning



Annexe 1 : Journal officiel de l'Union européenne – règlementation DSA

«

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)

LE PARLEMENT EUROPÉEN ET LE CONSEIL DE L'UNION EUROPÉENNE,

vu le traité sur le fonctionnement de l'Union européenne, et notamment son article 114,

vu la proposition de la Commission européenne,

après transmission du projet d'acte législatif aux parlements nationaux,

vu l'avis du Comité économique et social européen (1),

vu l'avis du Comité des régions (2),

statuant conformément à la procédure législative ordinaire (3),

considérant ce qui suit:

(1)

Les services de la société de l'information et surtout les services intermédiaires sont devenus une composante importante de l'économie de l'Union et de la vie quotidienne des citoyens de l'Union. Vingt ans après l'adoption du cadre juridique existant applicable à ces services, établi par la directive 2000/31/CE du Parlement européen et du Conseil (4), des services et des modèles économiques nouveaux et innovants, tels que les réseaux sociaux et les plateformes en ligne permettant aux consommateurs de conclure des contrats à distance avec des professionnels, ont permis aux utilisateurs professionnels et aux consommateurs de transmettre et d'accéder à l'information et d'effectuer des transactions de manière inédite. Une majorité de citoyens de l'Union utilise désormais ces services au quotidien. Toutefois, la transformation numérique et l'utilisation accrue de ces services ont également engendré de nouveaux risques et défis pour les différents destinataires des services concernés, pour les entreprises et pour la société dans son ensemble.

(2)

De plus en plus, les États membres adoptent ou envisagent d'adopter des législations nationales sur les matières relevant du présent règlement, imposant notamment des obligations de diligence aux fournisseurs de services intermédiaires en ce qui concerne la manière dont ils devraient combattre les contenus illicites, la désinformation en ligne ou d'autres risques pour la société. Étant donné le caractère intrinsèquement transfrontière de l'internet, qui est généralement utilisé pour fournir ces services, ces législations nationales

divergentes ont une incidence négative sur le marché intérieur qui, en vertu de l'article 26 du traité sur le fonctionnement de l'Union européenne, comporte un espace sans frontières intérieures dans lequel la libre circulation des marchandises et des services et la liberté d'établissement sont assurées. Les conditions de la prestation de services intermédiaires dans l'ensemble du marché intérieur devraient être harmonisées, de manière à permettre aux entreprises d'accéder à de nouveaux marchés et à de nouvelles possibilités d'exploiter les avantages du marché intérieur, tout en offrant un choix plus étendu aux consommateurs et aux autres destinataires des services. Les utilisateurs professionnels, les consommateurs et les autres utilisateurs sont considérés comme étant des «destinataires du service» aux fins du présent règlement.

(3)

Un comportement responsable et diligent des fournisseurs de services intermédiaires est indispensable pour assurer un environnement en ligne sûr, prévisible et fiable et pour permettre aux citoyens de l'Union et aux autres personnes d'exercer leurs droits fondamentaux garantis par la Charte des droits fondamentaux de l'Union européenne (ci-après dénommée «Charte»), en particulier la liberté d'expression et d'information, la liberté d'entreprise, le droit à la non-discrimination et la garantie d'un niveau élevé de protection des consommateurs.

(4)

Par conséquent, afin de préserver et d'améliorer le fonctionnement du marché intérieur, il convient d'établir un ensemble ciblé de règles obligatoires uniformes, efficaces et proportionnées au niveau de l'Union. Le présent règlement crée les conditions nécessaires à l'émergence et au développement de services numériques innovants dans le marché intérieur. Le rapprochement des mesures réglementaires nationales au niveau de l'Union relatives aux exigences applicables aux fournisseurs de services intermédiaires est nécessaire pour éviter et éliminer la fragmentation du marché intérieur et pour assurer la sécurité juridique, en réduisant par là même l'incertitude pour les développeurs et en favorisant l'interopérabilité. Grâce à des exigences neutres sur le plan technologique, l'innovation ne devrait pas être entravée, mais au contraire stimulée.

(5)

Le présent règlement devrait s'appliquer aux fournisseurs de certains services de la société de l'information tels qu'ils sont définis dans la directive (UE) 2015/1535 du Parlement européen et du Conseil (5), c'est-à-dire tout service fourni normalement contre rémunération, à distance, par voie électronique et à la demande individuelle d'un destinataire. Plus particulièrement, le présent règlement devrait s'appliquer aux fournisseurs de services intermédiaires, et notamment de services intermédiaires consistant en des services dits de «simple transport», de «mise en cache» et d'«hébergement», dès lors que la croissance exponentielle du recours à ces services, principalement à des fins légitimes et socialement bénéfiques de toute nature, a également accru leur rôle dans l'intermédiation et la diffusion d'informations et d'activités illégales ou susceptibles de nuire.

(6)

Dans la pratique, certains fournisseurs de services intermédiaires assurent une prestation d'intermédiaire pour des services qui peuvent ou non être fournis par voie électronique, tels que des services informatiques à distance ou des services de transport, de logement ou de livraison. Le présent règlement ne devrait s'appliquer qu'aux services intermédiaires et ne devrait pas porter atteinte aux exigences énoncées dans le droit de l'Union ou le droit national concernant les produits ou services fournis par le biais de services intermédiaires, y compris dans les situations où le service intermédiaire fait partie intégrante d'un autre service qui n'est pas un service intermédiaire, comme cela est établi dans la jurisprudence de la Cour de justice de l'Union européenne.

(7)

Afin de garantir l'efficacité des règles établies dans le présent règlement et l'existence de conditions de concurrence équitables au sein du marché intérieur, ces règles devraient s'appliquer aux fournisseurs de services intermédiaires, quel que soit leur lieu d'établissement ou leur situation géographique, dans la mesure où ils proposent des services dans l'Union, pour autant qu'un lien étroit avec l'Union soit avéré.

(8)

Il y a lieu de considérer qu'un tel lien étroit avec l'Union existe lorsque le fournisseur de services dispose d'un établissement dans l'Union ou, dans le cas contraire, lorsque le nombre de destinataires du service dans un ou plusieurs États membres est significatif au regard de leur population ou sur la base du ciblage des activités sur un ou plusieurs États membres. Le ciblage des activités sur un ou plusieurs États membres peut être déterminé sur la base de toutes les circonstances pertinentes, et notamment de facteurs comme l'utilisation d'une langue ou d'une monnaie généralement utilisées dans cet ou ces États membres, la possibilité de commander des produits ou des services, ou l'utilisation d'un domaine de premier niveau pertinent. Le ciblage des activités sur un État membre pourrait également se déduire de la disponibilité d'une application dans la boutique d'applications nationale concernée, de la diffusion de publicités à l'échelle locale ou dans une langue utilisée dans cet État membre, ou de la gestion des relations avec la clientèle, par exemple de la fourniture d'un service clientèle dans une langue utilisée généralement dans cet État membre. Un lien étroit devrait également être présumé lorsqu'un fournisseur de services dirige ses activités vers un ou plusieurs États membres au sens de l'article 17, paragraphe 1, point c), du règlement (UE) n° 1215/2012 du Parlement européen et du Conseil (6). En revanche, la simple accessibilité technique d'un site internet à partir de l'Union ne peut, pour ce seul motif, être considérée comme établissant un lien étroit avec l'Union.

(9)

Le présent règlement harmonise pleinement les règles applicables aux services intermédiaires dans le marché intérieur dans le but de garantir un environnement en ligne sûr, prévisible et de confiance, en luttant contre la diffusion de contenus illicites en ligne et contre les risques pour la société que la diffusion d'informations trompeuses ou d'autres contenus peuvent produire, et dans lequel les droits fondamentaux consacrés par la Charte sont efficacement protégés et l'innovation est facilitée. En conséquence, les États membres ne devraient pas adopter ou maintenir des exigences nationales supplémentaires concernant les matières relevant du champ d'application du présent règlement, sauf si le présent règlement le prévoit expressément, car cela porterait atteinte à l'application directe et uniforme des règles

pleinement harmonisées applicables aux fournisseurs de services intermédiaires conformément aux objectifs du présent règlement. Cela ne devrait pas empêcher l'application éventuelle d'une autre législation nationale applicable aux fournisseurs de services intermédiaires, dans le respect du droit de l'Union, y compris la directive 2000/31/CE, et notamment son article 3, lorsque les dispositions du droit national poursuivent d'autres objectifs légitimes d'intérêt général que ceux poursuivis par le présent règlement.

(10)

Il convient que le présent règlement soit sans préjudice d'autres actes du droit de l'Union régissant la fourniture de services de la société de l'information en général, régissant d'autres aspects de la fourniture de services intermédiaires dans le marché intérieur ou précisant et complétant les règles harmonisées énoncées dans le présent règlement, tels que la directive 2010/13/UE du Parlement européen et du Conseil (7), y compris les dispositions de ladite directive concernant les plateformes de partage de vidéos, les règlements (UE) 2019/1148 (8), (UE) 2019/1150 (9), (UE) 2021/784 (10) et (UE) 2021/1232 (11) du Parlement européen et du Conseil et la directive 2002/58/CE du Parlement européen et du Conseil (12) et les dispositions du droit de l'Union énoncées dans un règlement relatif aux injonctions européennes de production et de conservation de preuves électroniques en matière pénale et dans une directive établissant des règles harmonisées concernant la désignation de représentants légaux aux fins de la collecte de preuves en matière pénale.

De même, par souci de clarté, le présent règlement devrait être sans préjudice du droit de l'Union en matière de protection des consommateurs, en particulier les règlements (UE) 2017/2394 (13) et (UE) 2019/1020 (14) du Parlement européen et du Conseil, les directives 2001/95/CE (15), 2005/29/CE (16), 2011/83/UE (17) et 2013/11/UE (18) du Parlement européen et du Conseil et la directive 93/13/CEE du Conseil (19), et en matière de protection des données à caractère personnel, en particulier le règlement (UE) 2016/679 du Parlement européen et du Conseil (20).

Il convient également que le présent règlement soit sans préjudice des règles de l'Union en matière de droit international privé, en particulier les règles relatives à la compétence ainsi qu'à la reconnaissance et à l'exécution des décisions en matière civile et commerciale, comme le règlement (UE) n° 1215/2012, et les règles relatives à la loi applicable aux obligations contractuelles et non contractuelles. La protection des personnes au regard du traitement des données à caractère personnel est régie exclusivement par les règles du droit de l'Union en la matière, en particulier le règlement (UE) 2016/679 et la directive 2002/58/CE. Il convient également que le présent règlement soit sans préjudice du droit de l'Union relatif aux conditions de travail et du droit de l'Union dans le domaine de la coopération judiciaire en matière civile et pénale. Toutefois, dans la mesure où ces actes juridiques de l'Union poursuivent les mêmes objectifs que ceux énoncés dans le présent règlement, les règles du présent règlement devraient s'appliquer en ce qui concerne les aspects qui ne sont pas ou ne sont pas pleinement traités par ces autres actes juridiques ainsi que les aspects pour lesquels ces autres actes juridiques laissent aux États membres la possibilité d'adopter certaines mesures au niveau national.

(11)

Il convient de préciser que le présent règlement est sans préjudice du droit de l'Union sur le droit d'auteur et les droits voisins, y compris les directives 2001/29/CE (21), 2004/48/CE (22)

et (UE) 2019/790 (23) du Parlement européen et du Conseil, qui établissent des règles et des procédures spécifiques qui ne devraient pas être affectées.

(12)

Afin d'atteindre l'objectif consistant à garantir un environnement en ligne sûr, prévisible et fiable, il convient, aux fins du présent règlement, que la notion de «contenu illicite» corresponde de manière générale aux règles en vigueur dans l'environnement hors ligne. Il convient, en particulier, de donner une définition large de la notion de «contenu illicite» de façon à ce qu'elle couvre les informations relatives aux contenus, produits, services et activités illégaux. En particulier, cette notion devrait être comprise comme se référant à des informations, quelle que soit leur forme, qui, en vertu du droit applicable, sont soit elles-mêmes illicites, comme les discours haineux illégaux ou les contenus à caractère terroriste et les contenus discriminatoires illégaux, soit rendues illicites par les règles applicables en raison du fait qu'elles se rapportent à des activités illégales. Il peut s'agir, par exemple, du partage d'images représentant des abus sexuels commis sur des enfants, du partage illégal d'images privées sans consentement, du harcèlement en ligne, de la vente de produits non conformes ou contrefaits, de la vente de produits ou de la fourniture de services en violation du droit en matière de protection des consommateurs, de l'utilisation non autorisée de matériel protégé par le droit d'auteur, de l'offre illégale de services de logement ou de la vente illégale d'animaux vivants. En revanche, la vidéo d'un témoin oculaire d'une infraction pénale potentielle ne devrait pas être considérée comme constituant un contenu illicite simplement parce qu'elle met en scène un acte illégal, lorsque l'enregistrement ou la diffusion au public d'une telle vidéo n'est pas illégal en vertu du droit national ou du droit de l'Union. Il importe peu à cet égard que l'illégalité de l'information ou de l'activité procède du droit de l'Union ou du droit national conforme au droit de l'Union et il est indifférent de connaître la nature ou l'objet précis du droit en question.

(13)

Compte tenu des caractéristiques particulières des services concernés et de la nécessité qui en découle de soumettre leurs fournisseurs à certaines obligations spécifiques, il est nécessaire de distinguer, au sein de la catégorie plus large des fournisseurs de services d'hébergement telle qu'elle est définie dans le présent règlement, la sous-catégorie des plateformes en ligne. Les plateformes en ligne, telles que les réseaux sociaux ou les plateformes en ligne permettant aux consommateurs de conclure des contrats à distance avec des professionnels, devraient être définies comme des fournisseurs de services d'hébergement qui non seulement stockent les informations fournies par les destinataires du service à leur demande, mais qui diffusent également ces informations au public, à la demande des destinataires du service. Toutefois, afin d'éviter d'imposer des obligations trop étendues, les fournisseurs de services d'hébergement ne devraient pas être considérés comme des plateformes en ligne lorsque la diffusion au public n'est qu'une caractéristique mineure et purement accessoire qui est intrinsèquement liée à un autre service, ou une fonctionnalité mineure du service principal, et que cette caractéristique ou fonctionnalité ne peut, pour des raisons techniques objectives, être utilisée sans cet autre service ou ce service principal, et que l'intégration de cette caractéristique ou fonctionnalité n'est pas un moyen de se soustraire à l'applicabilité des règles du présent règlement relatives aux plateformes en ligne. Par exemple, la section «commentaires» d'un journal en ligne pourrait constituer une telle caractéristique, lorsqu'il est clair qu'elle est accessoire au service principal représenté par la publication d'actualités sous la responsabilité éditoriale de l'éditeur. En revanche, le stockage de commentaires sur un

réseau social devrait être considéré comme un service de plateforme en ligne lorsqu'il est clair qu'il ne constitue pas une caractéristique mineure du service offert, même s'il est accessoire à la publication des messages des destinataires du service. Aux fins du présent règlement, les services d'informatique en nuage ou les services d'hébergement de sites internet ne devraient pas être considérés comme une plateforme en ligne lorsque la diffusion d'informations spécifiques au public constitue une caractéristique mineure et accessoire ou une fonctionnalité mineure de ces services.

De plus, les services d'informatique en nuage et les services d'hébergement de sites internet qui servent d'infrastructure, par exemple les services de stockage et les services informatiques infrastructurels sous-jacents d'une application internet, d'un site internet ou d'une plateforme en ligne, ne devraient pas, en tant que tels, être considérés comme diffusant au public des informations stockées ou traitées à la demande d'un destinataire de l'application, du site internet ou de la plateforme en ligne qu'ils hébergent.

(14)

La notion de «diffusion au public», telle qu'elle est utilisée dans le présent règlement, devrait impliquer la mise à disposition de l'information à un nombre potentiellement illimité de personnes, c'est-à-dire le fait de rendre l'information facilement accessible aux destinataires du service en général sans que le destinataire du service ayant fourni l'information ait à intervenir, que ces personnes aient ou non effectivement accès à l'information en question. En conséquence, lorsque l'accès à une information nécessite un enregistrement ou l'admission au sein d'un groupe de destinataires du service, cette information ne devrait être considérée comme étant diffusée au public que lorsque les destinataires du service qui cherchent à accéder à cette information sont enregistrés ou admis automatiquement sans intervention humaine pour en décider ou pour sélectionner les personnes auxquelles l'accès est accordé. Les services de communication interpersonnelle, tels qu'ils sont définis dans la directive (UE) 2018/1972 du Parlement européen et du Conseil (24), comme les courriels ou les services de messagerie privée, ne relèvent pas du champ d'application de la définition des plateformes en ligne car ils sont utilisés pour la communication interpersonnelle entre un nombre fini de personnes, déterminé par l'émetteur de la communication. Cependant, les obligations prévues dans le présent règlement pour les fournisseurs de plateformes en ligne peuvent s'appliquer à des services qui permettent de mettre des informations à la disposition d'un nombre potentiellement illimité de destinataires, non déterminé par l'émetteur de la communication, notamment par l'intermédiaire de groupes publics ou de canaux ouverts. Des informations ne devraient être considérées comme étant diffusées au public au sens du présent règlement que lorsque cette diffusion se produit à la demande directe du destinataire du service qui a fourni les informations.

(15)

Lorsque certains des services fournis par un fournisseur sont couverts par le présent règlement alors que d'autres ne le sont pas, ou lorsque les services fournis par un fournisseur sont couverts par différentes sections du présent règlement, les dispositions pertinentes du présent règlement devraient s'appliquer uniquement aux services qui relèvent de leur champ d'application.

(16)

La sécurité juridique offerte par le cadre horizontal d'exemptions conditionnelles de responsabilité pour les fournisseurs de services intermédiaires, établi par la directive 2000/31/CE, a permis l'émergence et le développement de nombreux services nouveaux dans l'ensemble du marché intérieur. Il convient, dès lors, de conserver ce cadre. Toutefois, compte tenu des divergences dans la transposition et l'application des règles pertinentes au niveau national, et pour des raisons de clarté et de cohérence, il y a lieu d'intégrer ce cadre dans le présent règlement. Il est également nécessaire de clarifier certains éléments dudit cadre, compte tenu de la jurisprudence de la Cour de justice de l'Union européenne.

(17)

Les règles en matière de responsabilité des fournisseurs de services intermédiaires énoncées dans le présent règlement ne devraient établir que les cas dans lesquels le fournisseur de services intermédiaires concerné ne peut pas être tenu pour responsable du contenu illicite fourni par les destinataires du service. Ces règles ne devraient pas être interprétées comme constituant une base positive pour établir les cas dans lesquels la responsabilité d'un fournisseur peut être engagée, ce que les règles applicables du droit de l'Union ou du droit national doivent déterminer. En outre, les exemptions de responsabilité établies dans le présent règlement devraient s'appliquer à tout type de responsabilité à l'égard de tout type de contenu illicite, indépendamment de l'objet ou de la nature précis de ces législations.

(18)

Les exemptions de responsabilité établies dans le présent règlement ne devraient pas s'appliquer lorsque, au lieu de se limiter à fournir les services de manière neutre dans le cadre d'un simple traitement technique et automatique des informations fournies par le destinataire du service, le fournisseur de services intermédiaires joue un rôle actif de nature à lui permettre de connaître ou de contrôler ces informations. Ces exemptions ne devraient donc pas s'appliquer à la responsabilité relative aux informations fournies non pas par le destinataire du service, mais par le fournisseur du service intermédiaire lui-même, y compris lorsque les informations ont été établies sous la responsabilité éditoriale de ce fournisseur.

(19)

Compte tenu de la nature différente des activités de «simple transport», de «mise en cache» et d'«hébergement», ainsi que de la position et des capacités différentes des fournisseurs des services en question, il est nécessaire de distinguer les règles applicables à ces activités, dans la mesure où, dans le cadre du présent règlement, elles sont soumises à des exigences et à des conditions différentes et leur portée diffère, selon l'interprétation qu'en donne la Cour de justice de l'Union européenne.

(20)

Lorsqu'un fournisseur de services intermédiaires collabore délibérément avec un destinataire desdits services afin d'entreprendre des activités illégales, les services ne devraient pas être réputés avoir été fournis de manière neutre et le fournisseur ne devrait donc pas pouvoir bénéficier des exemptions de responsabilité prévues dans le présent règlement. Tel devrait être le cas, par exemple, lorsque le fournisseur propose son service dans le but principal de faciliter des activités illégales, par exemple en indiquant explicitement que son objectif est de faciliter des activités illégales ou que ses services sont adaptés à cette fin. Le seul fait qu'un

service propose des transmissions cryptées ou tout autre système rendant l'identification de l'utilisateur impossible ne devrait pas être considéré en soi comme facilitant des activités illégales.

(21)

Un fournisseur devrait pouvoir bénéficier des exemptions de responsabilité pour les services de «simple transport» et de «mise en cache» lorsqu'il n'est impliqué en aucune manière dans l'information transmise ou à laquelle il est donné accès. Cela suppose, entre autres, qu'il n'apporte pas de modification à l'information qu'il transmet ou à laquelle il donne accès. Cependant, cette exigence ne devrait pas être comprise comme couvrant les manipulations à caractère technique qui ont lieu au cours de la transmission ou de l'accès, tant que ces manipulations n'altèrent pas l'intégrité de l'information transmise ou à laquelle il est donné accès.

(22)

Afin de bénéficier de l'exemption de responsabilité relative aux services d'hébergement, le fournisseur devrait, dès qu'il a effectivement connaissance ou conscience d'une activité illégale ou d'un contenu illicite, agir rapidement pour retirer ce contenu ou rendre l'accès à ce contenu impossible. Il convient de retirer le contenu ou de rendre l'accès au contenu impossible dans le respect des droits fondamentaux des destinataires du service, y compris le droit à la liberté d'expression et d'information. Le fournisseur peut avoir effectivement connaissance ou prendre conscience du caractère illicite du contenu au moyen, entre autres, d'enquêtes effectuées de sa propre initiative ou de notifications qui lui sont soumises par des particuliers ou des entités conformément au présent règlement, dans la mesure où ces notifications sont assez précises et suffisamment étayées pour permettre à un opérateur économique diligent d'identifier et d'évaluer raisonnablement le contenu présumé illicite et, le cas échéant, d'agir contre celui-ci. Toutefois, cette connaissance ou prise de conscience effective ne peut être considérée comme étant présente au seul motif que le fournisseur est conscient, de manière générale, que son service est également utilisé pour stocker des contenus illicites. En outre, le fait qu'un fournisseur indexe automatiquement les informations mises en ligne sur son service, qu'il dispose d'une fonction de recherche ou qu'il recommande des informations sur la base des profils ou des préférences des destinataires du service ne constitue pas un motif suffisant pour considérer que ce fournisseur a "spécifiquement" connaissance des activités illégales menées sur cette plateforme ou des contenus illicites stockés sur celle-ci.

(23)

L'exemption de responsabilité ne devrait pas s'appliquer lorsque le destinataire du service agit sous l'autorité ou le contrôle du fournisseur d'un service d'hébergement. Par exemple, lorsque le fournisseur d'une plateforme en ligne qui permet aux consommateurs de conclure des contrats à distance avec des professionnels détermine le prix des biens ou services offerts par le professionnel, le professionnel pourrait être considéré comme agissant sous l'autorité ou le contrôle de ladite plateforme en ligne.

(24)

Afin d’assurer une protection efficace des consommateurs lorsqu’ils effectuent des transactions commerciales intermédiées en ligne, il convient que certains fournisseurs de services d’hébergement, à savoir les plateformes en ligne permettant aux consommateurs de conclure des contrats à distance avec des professionnels, ne bénéficient pas de l’exemption de responsabilité des fournisseurs de services d’hébergement établie dans le présent règlement, dans la mesure où ces plateformes en ligne présentent les informations pertinentes relatives aux transactions en cause de manière à conduire le consommateur à croire que les informations ont été fournies par ces plateformes en ligne elles-mêmes ou par des professionnels agissant sous leur autorité ou leur contrôle, et que ces plateformes en ligne ont donc connaissance de ces informations ou les contrôlent, même si ce n’est pas le cas en réalité. Des exemples de ce comportement pourraient être, lorsqu’une plateforme en ligne ne fait pas apparaître clairement l’identité du professionnel comme l’exige le présent règlement, lorsqu’elle retient l’identité ou les coordonnées du professionnel jusqu’à ce que le contrat entre le professionnel et le consommateur soit conclu ou lorsqu’elle commercialise le produit ou le service en son nom propre plutôt qu’au nom du professionnel qui fournira ce produit ou service. À cet égard, il convient de déterminer objectivement, sur la base de toutes les circonstances pertinentes, si la présentation est susceptible de conduire un consommateur moyen à croire que les informations en question ont été fournies par la plateforme en ligne elle-même ou par des professionnels agissant sous son autorité ou son contrôle.

(25)

Les exemptions de responsabilité établies dans le présent règlement ne devraient pas affecter la possibilité de procéder à des injonctions de différents types à l’encontre des fournisseurs de services intermédiaires, alors même qu’ils remplissent les conditions fixées dans le cadre de ces exemptions. Ces injonctions peuvent notamment revêtir la forme d’injonctions de juridictions ou d’autorités administratives, émises conformément au droit de l’Union, exigeant qu’il soit mis fin à toute infraction ou que l’on prévienne toute infraction, y compris en retirant les contenus illicites spécifiés dans ces injonctions, ou en rendant impossible l’accès à ces contenus.

(26)

Afin de créer une sécurité juridique et de ne pas décourager les activités visant à détecter, recenser et combattre les contenus illicites entreprises volontairement par les fournisseurs de toutes les catégories de services intermédiaires, il convient de préciser que le simple fait que les fournisseurs entreprennent de telles activités n’empêche pas le recours aux exemptions de responsabilité prévues par le présent règlement pour autant que ces activités soient menées de bonne foi et avec diligence. Il convient que la condition d’agir de bonne foi et avec diligence comprenne le fait d’agir de manière objective, non discriminatoire et proportionnée, en tenant dûment compte des droits et des intérêts légitimes de toutes les parties concernées, ainsi que le fait de fournir les garanties nécessaires contre la suppression injustifiée de contenus licites, conformément à l’objectif et aux exigences du présent règlement. À cette fin, il convient, par exemple, que les fournisseurs concernés prennent des mesures raisonnables pour garantir que, lorsque des outils automatisés sont utilisés pour mener de telles activités, la technologie concernée est suffisamment fiable pour limiter le plus possible le taux d’erreur. En outre, il convient de préciser que le simple fait que les fournisseurs prennent des mesures, de bonne foi, pour se conformer aux exigences du droit de l’Union, y compris celles énoncées dans le présent règlement en ce qui concerne la mise en œuvre de leurs conditions générales, ne devrait pas empêcher le recours aux exemptions de responsabilité prévues par le présent

règlement. Par conséquent, si de telles activités et mesures étaient prises par un fournisseur, elles ne devraient pas être prises en compte pour déterminer si ledit fournisseur peut se prévaloir d'une exemption de responsabilité, notamment en ce qui concerne la question de savoir s'il fournit son service de manière neutre et peut donc relever du champ d'application de la disposition concernée, cette règle n'impliquant cependant pas que ledit fournisseur peut nécessairement se prévaloir d'une exemption de responsabilité. Les actions volontaires ne sauraient servir à contourner les obligations incombant aux fournisseurs de services intermédiaires en vertu du présent règlement.

(27)

Alors que les règles sur la responsabilité des fournisseurs de services intermédiaires définies dans le présent règlement se concentrent sur l'exemption de responsabilité des fournisseurs de services intermédiaires, il est important de rappeler que, malgré le rôle généralement important joué par ces fournisseurs, le problème des contenus illicites et activités illégales en ligne ne devrait pas être traité sous le seul angle de leurs responsabilités. Dans la mesure du possible, les tiers affectés par des contenus illicites transmis ou stockés en ligne devraient tenter de résoudre les conflits relatifs à ces contenus sans impliquer les fournisseurs de services intermédiaires en question. Les destinataires du service devraient être tenus responsables des contenus illicites qu'ils fournissent et qu'ils peuvent diffuser au public par des services intermédiaires, lorsque les règles applicables du droit de l'Union et du droit national déterminant cette responsabilité le prévoient. Le cas échéant, d'autres acteurs, tels que les modérateurs de groupe dans des environnements en ligne fermés, notamment dans le cas de grands groupes, devraient également contribuer à éviter la diffusion de contenus illicites en ligne, conformément au droit applicable. En outre, lorsqu'il est nécessaire d'impliquer des fournisseurs de services de la société de l'information, y compris des fournisseurs de services intermédiaires, toute demande ou toute injonction concernant cette implication devrait, en règle générale, être adressée au fournisseur spécifique qui a la capacité technique et opérationnelle d'agir contre des éléments de contenus illicites particuliers, de manière à prévenir et à réduire au minimum tout effet négatif éventuel sur la disponibilité et l'accessibilité d'informations qui ne constituent pas des contenus illicites.

(28)

Depuis l'an 2000, de nouvelles technologies sont apparues qui améliorent la disponibilité, l'efficacité, la rapidité, la fiabilité, la capacité et la sécurité des systèmes de transmission, de "repérabilité" et de stockage des données en ligne, engendrant ainsi un écosystème en ligne de plus en plus complexe. À cet égard, il convient de rappeler que les fournisseurs de services établissant et facilitant l'architecture logique sous-jacente et le bon fonctionnement de l'internet, y compris les fonctions techniques accessoires, peuvent également bénéficier des exemptions de responsabilité prévues par le présent règlement, dans la mesure où leurs services peuvent être qualifiés de services de "simple transport", de "mise en cache" ou d'"hébergement". De tels services comprennent, le cas échéant, les réseaux locaux sans fil, les services de système de noms de domaine (DNS), les registres de noms de domaine de premier niveau, les bureaux d'enregistrement de noms de domaine, les autorités de certification qui délivrent des certificats numériques, les réseaux privés virtuels, les moteurs de recherche en ligne, les services d'infrastructure en nuage ou les réseaux d'acheminement de contenus qui permettent, localisent ou améliorent les fonctions d'autres fournisseurs de services intermédiaires. De même, les services utilisés à des fins de communication, et les moyens techniques de leur fourniture, ont également évolué de manière considérable, donnant

naissance à des services en ligne tels que la voix sur IP, les services de messagerie et les services de messagerie électronique sur l'internet, pour lesquels la communication est assurée via un service d'accès à l'internet. Ces services peuvent également bénéficier d'exemptions de responsabilité, dans la mesure où ils peuvent être qualifiés de services de "simple transport", de "mise en cache" ou d'"hébergement".

(29)

Les services intermédiaires couvrent un large éventail d'activités économiques qui ont lieu en ligne et évoluent en permanence pour permettre une transmission d'informations rapide, sûre et sécurisée, ainsi que pour garantir le confort de tous les participants à l'écosystème en ligne. À titre d'exemple, les services intermédiaires de "simple transport" comprennent des catégories génériques de services telles que les points d'échange internet, les points d'accès sans fil, les réseaux privés virtuels, les services de DNS et de résolution de noms de domaine, les registres de noms de domaine de premier niveau, les bureaux d'enregistrement de noms de domaine, les autorités de certification qui délivrent des certificats numériques, la voix sur IP et d'autres services de communication interpersonnelle, tandis que les exemples génériques de services intermédiaires de "mise en cache" comprennent la seule fourniture de réseaux d'acheminement de contenus, de serveurs mandataires inverses ou de serveurs mandataires d'adaptation de contenus. De tels services sont essentiels pour garantir la transmission fluide et efficace des informations fournies sur l'internet. Parmi les exemples de "services d'hébergement" figurent des catégories de services telles que l'informatique en nuage, l'hébergement de sites internet, les services de référencement payant ou les services permettant le partage d'informations et de contenus en ligne, y compris le stockage et le partage de fichiers. Les services intermédiaires peuvent être fournis isolément, dans le cadre d'un autre type de service intermédiaire, ou simultanément avec d'autres services intermédiaires. La question de savoir si un service spécifique constitue un service de "simple transport", de "mise en cache" ou d'"hébergement" dépend uniquement de ses fonctionnalités techniques, lesquelles sont susceptibles d'évoluer dans le temps, et devrait être appréciée au cas par cas.

(30)

Les fournisseurs de services intermédiaires ne devraient pas être soumis, ni de jure ni de facto, à une obligation de surveillance en ce qui concerne les obligations de nature générale. Cela ne concerne pas les obligations de surveillance dans un cas spécifique et, en particulier, cela n'affecte pas les injonctions émises par les autorités nationales conformément à la législation nationale, dans le respect du droit de l'Union, tel qu'il est interprété par la Cour de justice de l'Union européenne, et conformément aux conditions établies dans le présent règlement. Aucune disposition du présent règlement ne devrait être interprétée comme imposant une obligation générale de surveillance ou une obligation générale de recherche active des faits, ou comme une obligation générale, pour les fournisseurs, de prendre des mesures proactives à l'égard des contenus illicites.

(31)

En fonction du système juridique de chaque État membre et du domaine juridique en cause, les autorités judiciaires ou administratives nationales, y compris les autorités répressives, peuvent enjoindre aux fournisseurs de services intermédiaires de prendre des mesures à l'encontre d'un ou de plusieurs éléments de contenus illicites spécifiques ou de fournir

certaines informations spécifiques. Les législations nationales sur la base desquelles ces injonctions sont émises diffèrent considérablement et, de plus en plus souvent, les injonctions sont émises dans des contextes transfrontières. Afin de garantir le respect efficace et efficient de ces injonctions, en particulier dans un contexte transfrontière, de sorte que les autorités publiques concernées puissent accomplir leurs missions et que les fournisseurs ne soient pas soumis à des charges disproportionnées, sans porter indûment atteinte aux droits et intérêts légitimes de tiers, il est nécessaire de fixer certaines conditions auxquelles ces injonctions devraient répondre et certaines exigences complémentaires relatives au traitement de ces injonctions. En conséquence, le présent règlement devrait n'harmoniser que certaines conditions minimales spécifiques devant être respectées par ces injonctions pour donner naissance à l'obligation, pour les fournisseurs de services intermédiaires, d'informer les autorités concernées de la suite donnée à ces injonctions. Par conséquent, le présent règlement n'offre pas une base juridique pour l'émission de ces injonctions ni ne réglemente leur champ d'application territorial ou leur exécution transfrontière.

(32)

Le droit national ou de l'Union applicable sur la base duquel ces injonctions sont émises pourrait prévoir des conditions supplémentaires et devrait servir de base pour l'exécution des injonctions concernées. En cas de non-respect de ces injonctions, l'État membre d'émission devrait pouvoir les faire respecter conformément à son droit national. Les législations nationales applicables devraient être conformes au droit de l'Union, y compris à la Charte et aux dispositions du traité sur le fonctionnement de l'Union européenne relatives à la liberté d'établissement et à la libre prestation des services au sein de l'Union, en particulier en ce qui concerne les services en ligne de jeux d'argent et de hasard et de paris. De même, l'application de ces législations nationales aux fins de l'exécution des injonctions concernées s'entend sans préjudice des actes juridiques de l'Union ou des accords internationaux conclus par l'Union ou par les États membres concernant la reconnaissance, la mise en œuvre et l'exécution transfrontières de ces injonctions, en particulier en matière civile et pénale. Par ailleurs, il convient que l'exécution de l'obligation d'informer les autorités concernées de la suite donnée à ces injonctions, par opposition à l'exécution des injonctions elles-mêmes, soit soumise aux règles énoncées dans le présent règlement.

(33)

Il convient que le fournisseur de services intermédiaires informe l'autorité d'émission de toute suite donnée à ces injonctions, sans retard injustifié, dans le respect des délais prévus par le droit de l'Union ou le droit national applicable.

(34)

Les autorités nationales compétentes devraient pouvoir émettre de telles injonctions d'agir contre un contenu considéré comme illicite ou des injonctions de fournir des informations sur la base du droit de l'Union ou du droit national conforme au droit de l'Union, en particulier la Charte, et les adresser aux fournisseurs de services intermédiaires, y compris ceux qui sont établis dans un autre État membre. Le présent règlement devrait toutefois s'entendre sans préjudice du droit de l'Union dans le domaine de la coopération judiciaire en matière civile ou pénale, y compris le règlement (UE) n° 1215/2012 et un règlement relatif aux injonctions européennes de production et de conservation de preuves électroniques en matière pénale, et du droit de la procédure pénale ou du droit de la procédure civile national. Par conséquent,

lorsque ces législations prévoient, dans le cadre de procédures pénales ou civiles, des conditions supplémentaires à celles prévues dans le présent règlement ou incompatibles avec celles-ci en ce qui concerne les injonctions d'agir contre des contenus illicites ou de fournir des informations, les conditions prévues dans le présent règlement pourraient ne pas s'appliquer ou être adaptées. En particulier, l'obligation faite au coordinateur pour les services numériques de l'État membre de l'autorité d'émission de transmettre une copie des injonctions à tous les autres coordinateurs pour les services numériques pourrait ne pas s'appliquer dans le cadre de procédures pénales ou pourrait être adaptée, lorsque le droit de la procédure pénale national applicable le prévoit.

En outre, l'obligation pour les injonctions de contenir un exposé des motifs expliquant pourquoi l'information constitue un contenu illicite devrait être adaptée, si cela est nécessaire, en vertu du droit de la procédure pénale national applicable à des fins de prévention et de détection des infractions pénales et d'enquêtes et de poursuites en la matière. Enfin, l'obligation pour les fournisseurs de services intermédiaires d'informer le destinataire du service pourrait être différée conformément au droit de l'Union ou au droit national applicable, en particulier dans le cadre de procédures pénales, civiles ou administratives. En outre, les injonctions devraient être émises dans le respect du règlement (UE) 2016/679 et de l'interdiction des obligations générales de surveillance des informations ou de recherche active des faits ou des circonstances indiquant une activité illégale prévue par le présent règlement. Les conditions et exigences énoncées dans le présent règlement qui s'appliquent aux injonctions d'agir contre des contenus illicites sont sans préjudice d'autres actes de l'Union prévoyant des systèmes similaires visant à agir contre des types spécifiques de contenus illicites, tels que le règlement (UE) 2021/784, le règlement (UE) 2019/1020 ou le règlement (UE) 2017/2394 qui confère aux autorités des États membres chargées de faire respecter la législation en matière de protection des consommateurs des pouvoirs spécifiques pour ordonner la fourniture d'informations. De même, les conditions et exigences qui s'appliquent aux injonctions de fournir des informations sont sans préjudice d'autres actes de l'Union prévoyant des règles pertinentes similaires pour des secteurs spécifiques. Ces conditions et exigences devraient être sans préjudice des règles de conservation et de préservation prévues par le droit national applicable, en conformité avec le droit de l'Union et avec les demandes de traitement confidentiel concernant la non-divulgation d'informations émanant des autorités répressives. Ces conditions et exigences ne devraient pas faire obstacle à la possibilité, pour les États membres, d'exiger d'un fournisseur de services intermédiaires qu'il prévienne une infraction, en conformité avec le droit de l'Union, y compris le présent règlement, et en particulier avec l'interdiction des obligations générales de surveillance.

(35)

Il convient que les conditions et exigences fixées dans le présent règlement soient remplies au plus tard au moment de la transmission de l'injonction au fournisseur concerné. Par conséquent, l'injonction peut être émise dans l'une des langues officielles de l'autorité d'émission de l'État membre concerné. Toutefois, lorsque cette langue diffère de la langue déclarée par le fournisseur de services intermédiaires ou d'une autre langue officielle des États membres convenue entre l'autorité qui a émis l'injonction et le fournisseur de services intermédiaires, il convient que la transmission de l'injonction soit accompagnée d'une traduction, au minimum, des éléments de l'injonction qui sont prévus dans le présent règlement. Lorsqu'un fournisseur de services intermédiaires et les autorités d'un État membre sont convenus d'utiliser une certaine langue, il convient d'encourager ledit fournisseur à accepter des injonctions émises dans la même langue par les autorités d'autres États membres.

Il convient que les injonctions contiennent des éléments qui permettent au destinataire d'identifier l'autorité d'émission, y compris les coordonnées d'un point de contact au sein de ladite autorité, le cas échéant, et de vérifier le caractère authentique de l'injonction.

(36)

La portée territoriale de ces injonctions d'agir contre des contenus illicites devrait être clairement définie sur la base du droit de l'Union ou du droit national applicable en vertu duquel l'injonction est émise et ne devrait pas excéder ce qui est strictement nécessaire pour atteindre les objectifs de cette dernière. À cet égard, l'autorité judiciaire ou administrative nationale, qui pourrait être une autorité répressive, qui émet l'injonction devrait mettre en balance l'objectif poursuivi par l'injonction, conformément à la base juridique en vertu de laquelle elle est émise, et les droits et intérêts légitimes de l'ensemble des tiers susceptibles d'être affectés par celle-ci, en particulier leurs droits fondamentaux au titre de la Charte. En particulier dans un contexte transfrontière, l'effet de l'injonction devrait être, en principe, limité au territoire de l'État membre d'émission, à moins que le caractère illicite du contenu découle directement du droit de l'Union ou que l'autorité d'émission considère que les droits en cause requièrent un champ d'application territorial plus large, conformément au droit de l'Union et au droit international, en ce compris les impératifs de courtoisie internationale.

(37)

Les injonctions de fournir des informations régies par le présent règlement concernent la production d'informations spécifiques portant sur des destinataires particuliers du service intermédiaire concerné qui sont identifiés dans ces injonctions aux fins de déterminer si les destinataires du service respectent les règles de l'Union ou les règles nationales applicables. Il convient que ces injonctions demandent des informations destinées à permettre l'identification des destinataires du service concerné. Par conséquent, les injonctions relatives à des informations sur un groupe de destinataires du service qui ne sont pas précisément identifiés, y compris les injonctions de fournir des informations agrégées requises à des fins statistiques ou en vue de l'élaboration de politiques fondées sur des éléments factuels, ne sont pas couvertes par les exigences du présent règlement concernant la fourniture d'informations.

(38)

Les injonctions d'agir contre des contenus illicites et de fournir des informations ne sont soumises aux règles garantissant la compétence de l'État membre dans lequel le fournisseur de services visé est établi et aux règles prévoyant d'éventuelles dérogations à cette compétence dans certains cas, énoncées à l'article 3 de la directive 2000/31/CE, que si les conditions dudit article sont remplies. Dans la mesure où les injonctions en question portent, respectivement, sur des éléments de contenus illicites et sur des éléments d'information spécifiques, lorsqu'elles sont adressées à des fournisseurs de services intermédiaires établis dans un autre État membre, elles ne restreignent pas en principe la liberté de ces fournisseurs de fournir leurs services par-delà les frontières. Par conséquent, les règles énoncées à l'article 3 de la directive 2000/31/CE, y compris celles qui concernent la nécessité de justifier les mesures dérogeant à la compétence de l'État membre dans lequel le prestataire de services est établi pour certains motifs précis et la notification de ces mesures, ne s'appliquent pas à ces injonctions.

(39)

Les obligations de fournir des informations sur les mécanismes de recours dont disposent le fournisseur du service intermédiaire et le destinataire du service qui a fourni le contenu comprennent une obligation de fournir des informations sur les mécanismes administratifs de traitement des plaintes et les voies de recours juridictionnel, y compris les recours contre les injonctions émises par des autorités judiciaires. De plus, les coordinateurs pour les services numériques pourraient élaborer des outils et orientations nationaux en ce qui concerne les mécanismes de plainte et de recours applicables sur leur territoire respectif afin de faciliter l'accès des destinataires du service à ces mécanismes. Enfin, lors de l'application du présent règlement, il convient que les États membres respectent le droit fondamental à un recours juridictionnel effectif et à accéder à un tribunal impartial, comme le prévoit l'article 47 de la Charte. Le présent règlement ne devrait donc pas empêcher les autorités judiciaires ou administratives nationales compétentes, sur la base du droit de l'Union ou du droit national applicable, d'émettre une injonction de rétablir des contenus, lorsque ces contenus étaient conformes aux conditions générales du fournisseur de services intermédiaires, mais ont été considérés par erreur comme illicites par ce fournisseur et ont été retirés.

(40)

Afin d'atteindre les objectifs du présent règlement, et notamment d'améliorer le fonctionnement du marché intérieur et de garantir un environnement en ligne sûr et transparent, il est nécessaire d'établir un ensemble clair, efficace, prévisible et équilibré d'obligations harmonisées de diligence pour les fournisseurs de services intermédiaires. Ces obligations devraient notamment viser à garantir différents objectifs de politique publique, comme celui d'assurer la sécurité et la confiance des destinataires du service, y compris les consommateurs, les mineurs et les utilisateurs qui sont particulièrement exposés au risque de faire l'objet de discours haineux, de harcèlement sexuel ou d'autres actions discriminatoires, de protéger les droits fondamentaux concernés inscrits dans la Charte, d'assurer une véritable responsabilisation de ces fournisseurs et de donner les moyens d'agir aux destinataires et autres parties affectées, tout en facilitant le contrôle nécessaire par les autorités compétentes.

(41)

À cet égard, il est important que les obligations de diligence soient adaptées au type, à la taille et à la nature du service intermédiaire concerné. Le présent règlement définit donc des obligations de base applicables à tous les fournisseurs de services intermédiaires, ainsi que des obligations supplémentaires pour les fournisseurs de services d'hébergement et, plus particulièrement, pour les fournisseurs de plateformes en ligne et de très grandes plateformes en ligne ainsi que de très grands moteurs de recherche en ligne. Dans la mesure où les fournisseurs de services intermédiaires entrent dans un certain nombre de catégories différentes en raison de la nature de leurs services et de leur taille, ils devraient respecter toutes les obligations correspondantes du présent règlement se rapportant à ces services. Ces obligations harmonisées de diligence, qui devraient être raisonnables et non arbitraires, sont indispensables en vue de répondre aux préoccupations de politique publique déterminées, telles que la sauvegarde des intérêts légitimes des destinataires du service, la lutte contre les pratiques illégales et la protection des droits fondamentaux consacrés dans la Charte. Les obligations de diligence sont indépendantes de la question de la responsabilité des fournisseurs de services intermédiaires, qui doit donc être appréciée séparément.

(42)

Afin de faciliter une communication bidirectionnelle fluide et efficace, avec, le cas échéant, un accusé de réception de ladite communication, sur les matières relevant du présent règlement, les fournisseurs de services intermédiaires devraient être tenus de désigner un point de contact électronique unique et de publier et mettre à jour les informations utiles concernant ce point de contact, y compris les langues à utiliser dans cette communication. Le point de contact électronique peut également être utilisé par des signaleurs de confiance et par des entités professionnelles qui ont un lien particulier avec le fournisseur de services intermédiaires. Contrairement au représentant légal, le point de contact électronique devrait avoir une fonction opérationnelle et ne devrait pas être tenu d'avoir une localisation physique. Les fournisseurs de services intermédiaires peuvent désigner le même point de contact unique pour répondre aux exigences du présent règlement et aux fins d'autres actes du droit de l'Union. Lorsqu'ils spécifient les langues de communication, les fournisseurs de services intermédiaires sont encouragés à veiller à ce que les langues choisies ne constituent pas en elles-mêmes un obstacle à la communication. Si nécessaire, il devrait être possible pour les fournisseurs de services intermédiaires et les autorités des États membres de conclure un accord séparé sur la langue de communication, ou de chercher un autre moyen de surmonter la barrière linguistique, y compris en utilisant tous les moyens technologiques ou toutes les ressources humaines internes et externes disponibles.

(43)

Les fournisseurs de services intermédiaires devraient également être tenus de désigner un point de contact unique pour les destinataires des services, permettant d'établir une communication rapide, directe et efficace, en particulier par des moyens aisément accessibles, tels que des numéros de téléphone, des adresses de courrier électronique, des formulaires de contact électroniques, des dialogueurs ou des messageries instantanées. Lorsqu'un destinataire du service communique avec des dialogueurs, il convient de l'indiquer explicitement. Les fournisseurs de services intermédiaires devraient permettre aux destinataires des services de choisir des moyens de communication directe et efficace qui ne reposent pas uniquement sur des outils automatisés. Les fournisseurs de services intermédiaires devraient s'efforcer, dans la mesure du raisonnable, de garantir que des ressources humaines et financières suffisantes sont allouées pour que cette communication s'effectue de façon rapide et efficace.

(44)

Il convient que les fournisseurs de services intermédiaires établis dans un pays tiers qui proposent des services dans l'Union désignent un représentant légal doté d'un mandat suffisant dans l'Union et fournissent des informations relatives à leurs représentants légaux aux autorités compétentes et les mettent à la disposition du public. Pour se conformer à cette obligation, ces fournisseurs de services intermédiaires devraient veiller à ce que le représentant légal désigné dispose des pouvoirs et ressources nécessaires pour coopérer avec les autorités compétentes. Cela pourrait être le cas, par exemple, lorsqu'un fournisseur de services intermédiaires désigne une entreprise filiale du même groupe que lui, ou sa société mère, si cette entreprise filiale ou cette société mère est établie dans l'Union. Toutefois, cela pourrait ne pas être le cas, par exemple, lorsque le représentant légal fait l'objet d'une procédure d'assainissement, de faillite ou d'insolvabilité personnelle ou d'entreprise. Cette obligation devrait permettre un contrôle efficace et, si nécessaire, l'exécution du présent règlement à l'égard de ces fournisseurs. Il devrait être possible pour un représentant légal d'être mandaté, conformément au droit national, par plus d'un fournisseur de services

intermédiaires. Le représentant légal devrait pouvoir également faire office de point de contact, pour autant que les exigences pertinentes du présent règlement soient respectées.

(45)

Tout en respectant en principe la liberté contractuelle des fournisseurs de services intermédiaires, il convient de fixer certaines règles concernant le contenu, l'application et la mise en application des conditions générales de ces fournisseurs, dans un souci de transparence, de protection des destinataires du service et de prévention de conséquences inéquitables ou arbitraires. Les fournisseurs de services intermédiaires devraient indiquer clairement et tenir à jour dans leurs conditions générales les informations relatives aux motifs au titre desquels ils peuvent restreindre la fourniture de leurs services. Ils devraient en particulier inclure des renseignements ayant trait aux politiques, procédures, mesures et outils utilisés à des fins de modération des contenus, y compris la prise de décision fondée sur des algorithmes et le réexamen par un être humain ainsi que le règlement intérieur de leur système interne de traitement des réclamations. Ils devraient également fournir des informations aisément accessibles sur le droit de mettre fin à l'utilisation du service. Les fournisseurs de services intermédiaires peuvent utiliser des éléments graphiques dans leurs conditions générales, tels que des icônes ou des images, pour illustrer les principaux éléments des exigences en matière d'information énoncées dans le présent règlement. Les fournisseurs devraient informer les destinataires de leur service, à l'aide de moyens appropriés, au sujet des modifications importantes apportées aux conditions générales, par exemple lorsqu'ils modifient les règles relatives aux informations qui sont autorisées sur leur service, ou d'autres modifications de cette nature qui pourraient avoir une influence directe sur la capacité des destinataires à utiliser le service.

(46)

Les fournisseurs de services intermédiaires qui s'adressent principalement aux mineurs, par exemple par la conception ou la commercialisation du service, ou qui sont utilisés de manière prédominante par des mineurs, devraient déployer des efforts particuliers pour rendre l'explication de leurs conditions générales aisément compréhensible pour les mineurs.

(47)

Lorsqu'ils conçoivent, appliquent et font respecter ces restrictions, les fournisseurs de services intermédiaires devraient agir de manière non arbitraire et non discriminatoire et tenir compte des droits et des intérêts légitimes des destinataires du service, y compris les droits fondamentaux consacrés dans la Charte. Les fournisseurs de très grandes plateformes en ligne devraient, par exemple, en particulier, tenir dûment compte de la liberté d'expression et d'information, notamment la liberté et le pluralisme des médias. Tous les fournisseurs de services intermédiaires devraient également tenir dûment compte des normes internationales pertinentes en matière de protection des droits de l'homme, telles que les principes directeurs des Nations unies relatifs aux entreprises et aux droits de l'homme.

(48)

Compte tenu de leur portée et de leur rôle particuliers, il convient d'imposer aux très grandes plateformes en ligne et aux très grands moteurs de recherche en ligne des exigences supplémentaires en matière d'information et de transparence en ce qui concerne leurs

conditions générales. Par conséquent, les fournisseurs de très grandes plateformes en ligne ou de très grands moteurs de recherche en ligne devraient fournir leurs conditions générales dans les langues officielles de tous les États membres dans lesquels ils proposent leurs services et devraient également fournir aux destinataires des services un résumé concis et facilement lisible des principaux éléments des conditions générales. Ces résumés devraient recenser les principaux éléments des exigences en matière d'information, y compris la possibilité de ne pas consentir aux clauses optionnelles.

(49)

En vue de garantir un niveau adéquat de transparence et de responsabilisation, les fournisseurs de services intermédiaires devraient publier un rapport annuel dans un format lisible par une machine, conformément aux exigences harmonisées contenues dans le présent règlement, sur la modération des contenus à laquelle ils procèdent, y compris les mesures prises dans le cadre de l'application et de la mise en application de leurs conditions générales. Toutefois, afin d'éviter des charges disproportionnées, les obligations en matière de rapports de transparence ne devraient pas s'appliquer aux fournisseurs qui sont des microentreprises ou des petites entreprises telles qu'elles sont définies dans la recommandation 2003/361/CE de la Commission (25) et qui ne sont pas de très grandes plateformes en ligne au sens du présent règlement.

(50)

Les fournisseurs de services d'hébergement jouent un rôle particulièrement important dans la lutte contre les contenus illicites en ligne, car ils stockent les informations fournies par les destinataires du service et à la demande de ceux-ci, et permettent généralement à d'autres destinataires d'accéder à ces informations, parfois à grande échelle. Il est important que tous les fournisseurs de services d'hébergement, quelle que soit leur taille, mettent en place des mécanismes de notification et d'action facilement accessibles et faciles à utiliser, qui permettent de notifier aisément au fournisseur de services d'hébergement concerné les éléments d'information spécifiques que la partie notifiante considère comme un contenu illicite ("notification"), notification à la suite de laquelle ce fournisseur peut décider s'il est d'accord ou non avec cette évaluation et s'il souhaite ou non retirer ce contenu ou rendre l'accès à ce contenu impossible ("action"). Ces mécanismes devraient être clairement identifiables, situés à proximité des informations en question et au moins aussi faciles à trouver et à utiliser que les mécanismes de notification pour les contenus qui enfreignent les conditions générales du fournisseur de services d'hébergement. Pour autant que les exigences relatives aux notifications soient respectées, il devrait être possible à des particuliers ou à des entités de notifier plusieurs éléments spécifiques de contenus présumés illicites par le biais d'une notification unique afin de permettre la mise en œuvre effective des mécanismes de notification et d'action. Le mécanisme de notification devrait permettre, mais ne pas exiger, l'identification du particulier ou de l'entité soumettant la notification. Pour certains types d'éléments d'information notifiés, l'identité du particulier ou de l'entité soumettant la notification pourrait être nécessaire pour déterminer si les informations en question constituent un contenu illicite, comme il est allégué. L'obligation de mettre en place des mécanismes de notification et d'action devrait s'appliquer, par exemple, aux services de stockage et de partage de fichiers, aux services d'hébergement de sites internet, aux serveurs de publicité et aux "pastebins", dans la mesure où ils peuvent être qualifiés de services d'hébergement couverts par le présent règlement.

(51)

Eu égard à la nécessité de tenir dûment compte des droits fondamentaux de toutes les parties concernées garantis par la Charte, toute mesure prise par un fournisseur de services d'hébergement à la suite de la réception d'une notification devrait être strictement ciblée, au sens où elle devrait servir à retirer des éléments d'information spécifiques considérées comme constituant un contenu illicite ou à rendre l'accès à ceux-ci impossible, sans porter indûment atteinte à la liberté d'expression et d'information des destinataires du service. En conséquence, les notifications devraient, en règle générale, être adressées aux fournisseurs de services d'hébergement dont il peut être raisonnablement attendu qu'ils aient la capacité technique et opérationnelle d'agir contre ces éléments spécifiques. Les fournisseurs de services d'hébergement qui reçoivent une notification relative à un élément d'information spécifique qu'ils ne peuvent retirer, pour des raisons techniques ou opérationnelles, devraient en informer la personne ou l'entité qui a soumis la notification.

(52)

Il convient que les règles relatives à ces mécanismes de notification et d'action soient harmonisées au niveau de l'Union, de manière à permettre un traitement en temps utile, diligent et non arbitraire des notifications sur la base de règles uniformes, transparentes et claires et qui comportent des garanties solides protégeant les droits et intérêts légitimes de toutes les parties affectées, en particulier leurs droits fondamentaux garantis par la Charte, indépendamment de l'État membre dans lequel ces parties sont établies ou résident et du domaine juridique en cause. Ces droits fondamentaux comprennent notamment, sans s'y limiter: pour les destinataires du service, le droit à la liberté d'expression et d'information, le droit au respect de la vie privée et familiale, le droit à la protection des données à caractère personnel, le droit à la non-discrimination et le droit à un recours effectif; pour les fournisseurs de services, la liberté d'entreprise, y compris la liberté contractuelle; pour les parties affectées par un contenu illicite, le droit à la dignité humaine, les droits de l'enfant, le droit à la protection de la propriété, y compris la propriété intellectuelle, et le droit à la non-discrimination. Les fournisseurs de services d'hébergement devraient réagir rapidement aux notifications, notamment en tenant compte du type de contenu illicite notifié et de l'urgence d'agir. Il peut, par exemple, être attendu de ces fournisseurs qu'ils agissent sans retard en cas de notification d'un contenu présumé illicite comportant une menace pour la vie ou la sécurité des personnes. Le fournisseur de services d'hébergement devrait informer le particulier ou l'entité ayant notifié le contenu spécifique, sans retard injustifié après avoir pris la décision d'agir ou non à la suite de la notification.

(53)

Les mécanismes de notification et d'action devraient permettre la soumission de notifications suffisamment précises et dûment motivées pour permettre au fournisseur de services d'hébergement concerné de prendre une décision éclairée et diligente, compatible avec la liberté d'expression et d'information, en ce qui concerne le contenu auquel la notification se rapporte, en particulier la question de savoir si ce contenu doit ou non être considéré comme un contenu illicite et s'il doit être retiré ou si l'accès à ce contenu doit être rendu impossible. Ces mécanismes devraient être conçus de manière à faciliter l'envoi de notifications qui contiennent une explication des raisons pour lesquelles le particulier ou l'entité soumettant la notification considère le contenu comme un contenu illicite et une indication claire de l'emplacement du contenu en question. Lorsqu'une notification contient suffisamment

d’informations pour permettre à un fournisseur diligent de services d’hébergement de déterminer, sans examen juridique détaillé, que le contenu est clairement illicite, la notification devrait être réputée donner lieu à la connaissance ou à la prise de conscience effective de l’illégalité. À l’exception de la soumission de notifications relatives aux infractions visées aux articles 3 à 7 de la directive 2011/93/UE du Parlement européen et du Conseil (26), ces mécanismes devraient demander au particulier ou à l’entité soumettant la notification de divulguer son identité afin d’éviter toute utilisation abusive.

(54)

Lorsqu’un fournisseur de services d’hébergement décide, au motif que les informations fournies par le destinataire du service constituent du contenu illicite ou sont incompatibles avec ses conditions générales, de retirer des informations fournies par un destinataire du service ou de rendre impossible l’accès à de telles informations, ou de restreindre d’une autre manière leur visibilité ou leur monétisation, par exemple à la suite de la réception d’une notification ou de sa propre initiative, y compris par l’utilisation exclusive d’outils automatisés, il convient que ce fournisseur informe le destinataire, de manière claire et facilement compréhensible, de sa décision, des raisons de celle-ci et des possibilités de recours disponibles pour la contester, compte tenu des conséquences négatives que de telles décisions peuvent avoir pour le destinataire, y compris en ce qui concerne l’exercice de son droit fondamental à la liberté d’expression. Cette obligation devrait s’appliquer quelles que soient les raisons de la décision, en particulier si l’action a été engagée parce que les informations notifiées sont considérées comme un contenu illicite ou sont incompatibles avec les conditions générales applicables au service. Lorsque la décision a été prise à la suite de la réception d’une notification, le fournisseur de services d’hébergement ne devrait révéler l’identité de la personne ou de l’entité qui a soumis la notification au destinataire du service que lorsque cette information est nécessaire pour déterminer l’illicéité du contenu, par exemple en cas de violation des droits de propriété intellectuelle.

(55)

La restriction de la visibilité peut prendre la forme d’une rétrogradation dans les systèmes de classement ou de recommandation, ainsi que d’une limitation de l’accessibilité pour un ou plusieurs destinataires du service ou du blocage de l’utilisateur sur une communauté en ligne à l’insu de ce dernier (“bannissement par l’ombre”). La monétisation via les recettes publicitaires générées par les informations fournies par le destinataire du service peut être restreinte au moyen de la suspension ou la fin des paiements monétaires ou des recettes associées aux informations concernées. L’obligation de fournir un exposé des motifs ne devrait toutefois pas s’appliquer aux contenus commerciaux trompeurs et de grande diffusion diffusés par manipulation intentionnelle du service, en particulier l’utilisation non authentique du service, comme l’utilisation de robots ou de faux comptes ou d’autres utilisations trompeuses du service. Quelles que soient les autres possibilités de contester la décision du fournisseur de services d’hébergement, le destinataire du service devrait toujours disposer d’un droit de recours effectif devant une juridiction, conformément au droit national.

(56)

Un fournisseur de services d’hébergement peut, dans certains cas, avoir connaissance, à la suite de la notification d’une partie notifiante ou des mesures qu’il a lui-même volontairement adoptées, d’informations relatives à certaines activités d’un destinataire du service, telles que

la fourniture de certains types de contenus illicites, qui donnent lieu à des motifs raisonnables de soupçonner, compte tenu de toutes les circonstances pertinentes dont le fournisseur de services d'hébergement a connaissance, que ce destinataire peut avoir commis, peut être en train de commettre ou est susceptible de commettre une infraction pénale impliquant une menace pour la vie ou la sécurité d'une ou de plusieurs personnes, telles que des infractions définies dans la directive 2011/36/UE du Parlement européen et du Conseil (27), dans la directive 2011/93/UE ou dans la directive (UE) 2017/541 du Parlement européen et du Conseil (28). À titre d'exemple, des éléments spécifiques de contenus peuvent conduire à soupçonner l'existence d'une menace pour le public, telle que la provocation à commettre une infraction terroriste au sens de l'article 21 de la directive (UE) 2017/541. Dans de tels cas, le fournisseur de services d'hébergement devrait informer sans retard les autorités répressives compétentes de tels soupçons. Le fournisseur de services d'hébergement devrait fournir toutes les informations pertinentes dont il dispose, en particulier, le cas échéant, le contenu en question et, s'il est connu, le moment où il a été publié, y compris le fuseau horaire désigné, une explication quant à ses soupçons et les informations nécessaires pour localiser et identifier le destinataire du service concerné. Le présent règlement n'offre pas de base juridique pour le profilage des destinataires des services aux fins de la détection éventuelle d'infractions pénales par les fournisseurs de services d'hébergement. Les fournisseurs de services d'hébergement devraient également respecter les autres dispositions applicables du droit de l'Union ou du droit national relatives à la protection des droits et libertés des personnes lorsqu'ils informent les autorités répressives.

(57)

Pour éviter d'imposer des contraintes disproportionnées, les obligations supplémentaires imposées au titre du présent règlement aux fournisseurs de plateformes en ligne, y compris les plateformes permettant aux consommateurs de conclure des contrats à distance avec des professionnels, ne devraient pas s'appliquer aux fournisseurs qui peuvent être qualifiés de microentreprises ou de petites entreprises telles qu'elles sont définies dans la recommandation 2003/361/CE. Pour la même raison, ces obligations supplémentaires ne devraient pas non plus s'appliquer aux fournisseurs de plateformes en ligne qui étaient qualifiés précédemment de microentreprises ou de petites entreprises, pendant une période de douze mois suivant la perte de ce statut. Ces fournisseurs ne devraient pas être exclus de l'obligation de fournir des informations sur la moyenne mensuelle des destinataires actifs du service à la demande du coordinateur pour les services numériques de l'État membre d'établissement ou de la Commission. Toutefois, étant donné que les très grandes plateformes en ligne ou les très grands moteurs de recherche en ligne ont une plus grande portée et une plus grande influence sur la manière dont les destinataires du service obtiennent des informations et communiquent en ligne, ces fournisseurs ne devraient pas bénéficier de cette exclusion, indépendamment du fait qu'ils soient qualifiés de microentreprises ou de petites entreprises ou qu'ils aient été récemment qualifiés comme tels. Les règles de consolidation fixées dans la recommandation 2003/361/CE contribuent à prévenir tout contournement de ces obligations supplémentaires. Aucune disposition du présent règlement n'empêche les fournisseurs de plateformes en ligne couverts par cette exclusion de mettre en place, sur une base volontaire, un système qui respecte une ou plusieurs de ces obligations.

(58)

Les destinataires du service devraient pouvoir contester facilement et efficacement certaines décisions des fournisseurs de plateformes en ligne, relatives à l'illicéité d'un contenu ou à son

incompatibilité avec les conditions générales, qui ont une incidence négative pour eux. Il convient donc que les fournisseurs de plateformes en ligne soient tenus de prévoir des systèmes internes de traitement des réclamations, qui remplissent certaines conditions visant à garantir la facilité d'accès à ces systèmes ainsi que leur capacité d'aboutir à des résultats rapides, non discriminatoires, non arbitraires et équitables, et à garantir que ces systèmes fassent l'objet d'un réexamen par un être humain lorsque des moyens automatisés sont utilisés. Ces systèmes devraient permettre à tous les destinataires du service d'introduire une réclamation et ne devraient pas fixer d'exigences formelles, telles que le renvoi à des dispositions juridiques spécifiques pertinentes ou à des explications juridiques compliquées. Les destinataires du service qui ont soumis une notification, au moyen du mécanisme de notification et d'action prévu par le présent règlement ou par l'intermédiaire du mécanisme de notification des contenus qui enfreignent les conditions générales du fournisseur de plateformes en ligne, devraient être autorisés à utiliser le mécanisme de réclamation pour contester la décision du fournisseur de plateformes en ligne concernant leurs notifications, y compris lorsqu'ils estiment que les mesures prises par ce fournisseur n'étaient pas adéquates. La possibilité d'introduire une réclamation visant à obtenir l'annulation de la décision contestée devrait être disponible pendant au moins six mois, à compter du moment auquel le fournisseur de plateformes en ligne a informé le destinataire du service de la décision.

(59)

En outre, il convient de prévoir la possibilité de participer de bonne foi à un règlement extrajudiciaire de ces litiges, y compris de ceux qui n'ont pas pu être résolus de manière satisfaisante par les systèmes internes de traitement des réclamations, par des organes certifiés qui disposent de l'indépendance, des moyens et de l'expertise nécessaires pour s'acquitter de leur mission d'une manière équitable, rapide et économiquement avantageuse. L'indépendance des organes de règlement extrajudiciaire des litiges devrait également être garantie au niveau des personnes physiques chargées de régler les litiges, y compris au moyen de règles sur les conflits d'intérêts. Les frais facturés par les organes de règlement extrajudiciaire des litiges devraient être raisonnables, abordables, attrayants, peu coûteux pour les consommateurs et proportionnés et devraient être évalués au cas par cas. Lorsqu'un organe de règlement extrajudiciaire des litiges est certifié par le coordinateur pour les services numériques compétent, ce certificat devrait être valide dans tous les États membres. Les fournisseurs de plateformes en ligne devraient pouvoir refuser de participer à des procédures de règlement extrajudiciaire des litiges au titre du présent règlement lorsque le même litige, en particulier en ce qui concerne les informations concernées et les motifs de la décision attaquée, les effets de la décision et les motifs invoqués pour contester la décision, a déjà été résolu par une procédure en cours devant la juridiction compétente ou devant un autre organe de règlement extrajudiciaire des litiges compétent ou fait déjà l'objet d'une procédure en cours devant une telle juridiction ou un tel organe. Les destinataires du service devraient pouvoir choisir entre le mécanisme interne de traitement des réclamations, un règlement extrajudiciaire des litiges et la possibilité d'engager, à tout moment, une procédure juridictionnelle. Étant donné que l'issue de la procédure de règlement extrajudiciaire des litiges n'est pas contraignante, les parties ne devraient pas être empêchées d'engager une procédure judiciaire concernant le même litige. Les possibilités de contester les décisions des fournisseurs de plateformes en ligne ne devraient altérer en aucune manière la possibilité de former un recours juridictionnel conformément à la législation de l'État membre concerné, et ne sauraient donc porter atteinte à l'exercice du droit à un recours juridictionnel effectif tel qu'il est prévu à l'article 47 de la Charte. Les dispositions du présent règlement relatives au

règlement extrajudiciaire des litiges ne devraient pas obliger les États membres à mettre en place de tels organes de règlement extrajudiciaire des litiges.

(60)

Pour les litiges contractuels entre consommateurs et entreprises concernant l'achat de biens ou de services, la directive 2013/11/UE garantit que les consommateurs et les entreprises de l'Union ont accès à des entités de règlement extrajudiciaire des litiges dont la qualité est certifiée. À cet égard, il convient de préciser que les règles du présent règlement relatives au règlement extrajudiciaire des litiges sont sans préjudice de ladite directive, y compris du droit qu'elle confère aux consommateurs de se retirer de la procédure à tout moment s'ils sont insatisfaits du déroulement ou du fonctionnement de la procédure.

(61)

Il est possible d'agir plus rapidement et de manière plus fiable contre les contenus illicites lorsque les fournisseurs de plateformes en ligne prennent les mesures nécessaires pour faire en sorte que les notifications soumises par des signaleurs de confiance, qui agissent dans leur domaine d'expertise désigné, par l'intermédiaire des mécanismes de notification et d'action requis par le présent règlement soient traitées en priorité, sans préjudice de l'obligation de traiter et de statuer sur toutes les notifications soumises dans le cadre de ces mécanismes, en temps utile, avec diligence et de manière non arbitraire. Ce statut de signaleur de confiance devrait être attribué par le coordinateur pour les services numériques de l'État membre dans lequel l'entité présentant la demande est établie, et il devrait être reconnu par tous les fournisseurs de plateformes en ligne relevant du champ d'application du présent règlement. Ce statut de signaleur de confiance ne devrait être attribué qu'aux entités, et non aux particuliers, qui ont démontré, entre autres, qu'elles possèdent une expertise et une compétence particulières dans la lutte contre les contenus illicites et qu'elles travaillent de manière diligente, précise et objective. Il peut s'agir d'entités publiques, comme, en ce qui concerne les contenus terroristes, les unités de signalement des contenus sur l'internet des autorités répressives nationales ou de l'Agence de l'Union européenne pour la coopération des services répressifs (Europol), ou il peut s'agir d'organisations non gouvernementales et d'organismes privés ou semi-publics, tels que les organisations faisant partie du réseau INHOPE de permanences téléphoniques pour le signalement de matériel pédopornographique et les organisations ayant pour objectif de signaler les expressions racistes et xénophobes illégales en ligne. Pour éviter de diminuer la valeur ajoutée d'un tel mécanisme, le nombre total de signaleurs de confiance reconnus conformément au présent règlement devrait être limité. En particulier, les associations professionnelles représentant les intérêts de leurs membres sont encouragées à demander le statut de signaleurs de confiance, sans préjudice du droit des entités privées ou des particuliers de conclure des accords bilatéraux avec les fournisseurs de plateformes en ligne.

(62)

Les signaleurs de confiance devraient publier des rapports facilement compréhensibles et détaillés sur les notifications soumises conformément au présent règlement. Ces rapports devraient indiquer des informations telles que le nombre de notifications classées par fournisseur de services d'hébergement, type de contenu et action entreprise par le fournisseur. Étant donné que les signaleurs de confiance ont fait la preuve de leur expertise et de leur compétence, il peut être escompté que le traitement des notifications provenant de signaleurs

de confiance soit moins contraignant et donc plus rapide que celui des notifications émanant d'autres destinataires du service. Cependant, le temps moyen nécessaire pour traiter les notifications peut toujours varier en fonction de facteurs tels que le type de contenu illicite, la qualité des notifications et les procédures techniques concrètes mises en place pour la soumission de ces notifications.

Par exemple, si le code de conduite pour la lutte contre les discours haineux illégaux en ligne de 2016 fixe un critère de référence pour les entreprises participantes en ce qui concerne le temps nécessaire au traitement des notifications valides en vue du retrait de discours haineux illégaux, d'autres types de contenus illicites peuvent prendre des délais de traitement très différents, en fonction des faits et circonstances spécifiques et des types de contenus illicites en jeu. Afin d'éviter les abus du statut de signaleur de confiance, il devrait être possible de suspendre ce statut lorsqu'un coordinateur pour les services numériques de l'État membre d'établissement a ouvert une enquête pour des raisons légitimes. Les dispositions du présent règlement relatives aux signaleurs de confiance ne devraient pas être interprétées comme empêchant les fournisseurs de plateformes en ligne de traiter de la même manière les notifications soumises par des entités ou des particuliers auxquels le statut de signaleur de confiance prévu par le présent règlement n'a pas été accordé, ou de coopérer d'une autre manière avec d'autres entités, conformément au droit applicable, notamment le présent règlement et le règlement (UE) 2016/794 du Parlement européen et du Conseil (29). Les dispositions du présent règlement ne devraient pas empêcher les fournisseurs de plateformes en ligne d'utiliser ce mécanisme de signaleurs de confiance ou des mécanismes similaires pour prendre des mesures rapides et fiables contre les contenus qui sont incompatibles avec leurs conditions générales, en particulier contre les contenus qui sont préjudiciables aux destinataires vulnérables du service, tels que les mineurs.

(63)

Utiliser de manière abusive les plateformes en ligne en fournissant fréquemment des contenus manifestement illicites ou en soumettant souvent des notifications ou des réclamations manifestement infondées dans le cadre, respectivement, des mécanismes et systèmes mis en place en vertu du présent règlement nuit à la confiance et porte atteinte aux droits et intérêts légitimes des parties concernées. Il est donc nécessaire de mettre en place des garanties appropriées, proportionnées et efficaces contre de tels abus, garanties qui doivent respecter les droits et les intérêts légitimes de toutes les parties concernées, y compris les libertés et droits fondamentaux applicables consacrés par la Charte, en particulier la liberté d'expression. Il convient de considérer des informations comme des contenus manifestement illicites et des notifications ou réclamations comme manifestement infondées lorsqu'il est évident pour un profane, sans aucune analyse de fond, que le contenu est illicite ou que les notifications ou réclamations sont infondées, respectivement.

(64)

Sous certaines conditions, les fournisseurs de plateformes en ligne devraient suspendre temporairement leurs activités pertinentes concernant la personne ayant un comportement abusif. Cela s'entend sans préjudice de la liberté des fournisseurs de plateformes en ligne de déterminer leurs conditions générales et d'établir des mesures plus strictes dans le cas de contenus manifestement illicites liés à des infractions graves, tels que le matériel pédopornographique. Pour des raisons de transparence, il convient que les conditions générales des plateformes en ligne fassent clairement état, et de manière suffisamment

détaillée, de cette possibilité. Les décisions prises à cet égard par les fournisseurs de plateformes en ligne devraient toujours être susceptibles de recours et elles devraient être soumises au contrôle du coordinateur pour les services numériques compétent. Avant de décider de procéder à une suspension, les fournisseurs de plateformes en ligne devraient envoyer un avertissement préalable, qui devrait préciser les motifs de l'éventuelle suspension et les voies de recours disponibles contre leur décision. Lorsqu'ils décident de procéder à une suspension, les fournisseurs de plateformes en ligne devraient envoyer l'exposé des motifs conformément aux dispositions énoncées dans le présent règlement. Les règles du présent règlement relatives aux utilisations abusives ne devraient pas empêcher les fournisseurs de plateformes en ligne de prendre d'autres mesures pour lutter contre la fourniture de contenus illicites par les destinataires de leurs services ou contre tout autre usage abusif de leurs services, y compris par la violation de leurs conditions générales, conformément au droit de l'Union et au droit national applicables. Ces règles ne portent pas atteinte à la possibilité de tenir les personnes se livrant à une utilisation abusive pour responsables, notamment des dommages, conformément au droit de l'Union ou au droit national.

(65)

Compte tenu des responsabilités et obligations particulières des fournisseurs de plateformes en ligne, il convient de les soumettre à des obligations en matière de rapports de transparence, qui s'appliquent en sus des obligations en matière de rapports de transparence imposées à tous les fournisseurs de services intermédiaires par le présent règlement. Afin de déterminer si des plateformes en ligne et des moteurs de recherche en ligne sont susceptibles d'être, respectivement, de très grandes plateformes en ligne ou de très grands moteurs de recherche en ligne soumis à certaines obligations supplémentaires par le présent règlement, les obligations en matière de rapports de transparence applicables aux plateformes en ligne et aux moteurs de recherche en ligne devraient inclure certaines obligations relatives à la publication et à la communication d'informations sur le nombre mensuel moyen de destinataires actifs du service dans l'Union.

(66)

En vue de garantir la transparence et de permettre le contrôle des décisions relatives à la modération des contenus des fournisseurs de plateformes en ligne et le suivi de la diffusion de contenus illicites en ligne, il convient que la Commission gère et publie une base de données contenant les décisions et les exposés des motifs des fournisseurs de plateformes en ligne lorsqu'ils retirent des informations ou limitent d'une autre manière la disponibilité d'informations et l'accès à des informations. Afin de maintenir la base de données constamment à jour, les fournisseurs de plateformes en ligne devraient soumettre, dans un format standard, les décisions et les exposés des motifs sans retard injustifié après avoir pris une décision, afin de permettre des mises à jour en temps réel lorsque cela est techniquement possible et proportionné aux moyens de la plateforme en ligne en question. La base de données structurée devrait permettre d'accéder aux informations pertinentes et de les rechercher, notamment en ce qui concerne le type de contenus présumés illicites en jeu.

(67)

Les interfaces en ligne trompeuses de plateformes en ligne sont des pratiques qui ont pour objectif ou pour effet d'altérer ou d'entraver sensiblement la capacité des destinataires du service de prendre une décision ou de faire un choix, de manière autonome et éclairée. Ces

pratiques peuvent être utilisées pour persuader les destinataires du service de se livrer à des comportements non désirés ou de prendre des décisions non souhaitées qui ont des conséquences négatives pour eux. Par conséquent, il devrait être interdit pour les fournisseurs de plateformes en ligne de tromper ou d'encourager dans un sens les destinataires du service et d'altérer ou d'entraver l'autonomie, la prise de décision ou le choix des destinataires du service par la structure, la conception ou les fonctionnalités d'une interface en ligne ou d'une partie de celle-ci. Cela devrait comprendre, sans s'y limiter, les choix de conception abusifs destinés à amener le destinataire à exécuter des actions qui profitent au fournisseur de plateformes en ligne mais qui ne sont pas nécessairement dans l'intérêt du destinataire, en lui présentant des choix de manière biaisée, par exemple en accordant davantage d'importance à certains choix au moyen de composantes visuelles, auditives ou autres, lorsqu'il est demandé au destinataire du service de prendre une décision.

Cela devrait également inclure le fait de demander à plusieurs reprises à un destinataire du service de faire un choix lorsque ce choix a déjà été fait, de rendre la procédure d'annulation d'un service nettement plus compliquée que celle de s'y inscrire, de rendre certains choix plus difficiles ou plus longs que d'autres, de rendre excessivement difficile l'interruption des achats ou le fait de quitter une plateforme en ligne donnée permettant aux consommateurs de conclure des contrats à distance avec des professionnels, de tromper les destinataires du service en les incitant à prendre des décisions sur des transactions, ou d'appliquer des paramètres par défaut très difficiles à modifier, et d'influencer ainsi de manière excessive la prise de décision des destinataires du service, d'une manière qui altère et entrave leur autonomie, leur prise de décision et leur choix. Toutefois, les règles qui empêchent les interfaces trompeuses ne devraient pas être interprétées comme empêchant les fournisseurs d'interagir directement avec les destinataires du service et de leur proposer des services nouveaux ou supplémentaires. Les pratiques légitimes, par exemple dans le domaine de la publicité, qui sont conformes au droit de l'Union ne devraient pas en elles-mêmes être considérées comme constituant des interfaces trompeuses. Ces règles relatives aux interfaces trompeuses devraient être interprétées comme couvrant les pratiques interdites relevant du champ d'application du présent règlement dans la mesure où ces pratiques ne sont pas déjà couvertes par la directive 2005/29/CE ou le règlement (UE) 2016/679.

(68)

La publicité en ligne joue un rôle important dans l'environnement en ligne, notamment en ce qui concerne la fourniture de plateformes en ligne, où la fourniture du service est parfois rémunérée, en tout ou en partie, directement ou indirectement, au moyen de recettes publicitaires. La publicité en ligne peut présenter des risques importants, qu'il s'agisse de messages publicitaires constituant eux-mêmes un contenu illicite, de la contribution à des incitations financières en faveur de la publication ou de l'amplification de contenus et d'activités illégales ou autrement préjudiciables en ligne, ou encore de la présentation discriminatoire de publicités ayant une incidence sur l'égalité de traitement et des chances des citoyens. Outre les exigences découlant de l'article 6 de la directive 2000/31/CE, il convient donc que les fournisseurs de plateformes en ligne soient tenus de veiller à ce que les destinataires du service disposent de certaines informations individualisées qui leur sont nécessaires pour comprendre quand et pour le compte de qui la publicité est présentée. Ils devraient veiller à ce que les informations soient bien visibles, notamment grâce à des signes visuels ou sonores standardisés, clairement identifiables et dépourvues d'ambiguïté pour le destinataire moyen du service, et à ce qu'elles soient adaptées à la nature de l'interface en ligne du service individuel. De plus, les destinataires du service devraient disposer

d’informations, directement accessibles depuis l’interface en ligne lorsque la publicité est présentée, relatives aux principaux paramètres utilisés pour déterminer qu’une publicité spécifique leur est présentée, accompagnées d’explications judicieuses sur la logique utilisée à cette fin, notamment lorsque celle-ci est fondée sur le profilage.

Ces explications devraient comprendre des informations sur la méthode utilisée pour présenter la publicité, par exemple préciser s’il s’agit d’une publicité contextuelle ou d’un autre type de publicité et, le cas échéant, les principaux critères de profilage utilisés; elles devraient également informer le destinataire de tout moyen dont il dispose pour modifier ces critères. Les exigences du présent règlement concernant la fourniture d’informations relatives à la publicité sont sans préjudice de l’application des dispositions pertinentes du règlement (UE) 2016/679, en particulier celles relatives au droit d’opposition, à la prise de décision individuelle automatisée, y compris le profilage, et en particulier à la nécessité d’obtenir le consentement de la personne concernée avant de traiter des données à caractère personnel à des fins de publicité ciblée. De même, elles sont sans préjudice des dispositions prévues par la directive 2002/58/CE, notamment celles qui concernent le stockage d’informations dans les équipements terminaux et l’accès aux informations qui y sont stockées. Enfin, le présent règlement complète l’application de la directive 2010/13/UE, qui impose des mesures pour permettre aux utilisateurs de déclarer les communications commerciales audiovisuelles figurant dans les vidéos qu’ils ont créées. Il complète également les obligations imposées aux professionnels en vertu de la directive 2005/29/CE concernant la divulgation des communications commerciales.

(69)

Lorsque les destinataires du service reçoivent des publicités fondées sur des techniques de ciblage optimisées pour répondre à leurs intérêts et potentiellement exploiter leurs vulnérabilités, cela peut avoir des effets négatifs particulièrement graves. Dans certains cas, les techniques de manipulation peuvent avoir une incidence négative sur des groupes entiers et amplifier les préjudices sociétaux, par exemple en contribuant à des campagnes de désinformation ou en pratiquant des discriminations à l’égard de certains groupes. Les plateformes en ligne sont des environnements particulièrement sensibles pour de telles pratiques et présentent un risque plus élevé pour la société. Par conséquent, les fournisseurs de plateformes en ligne ne devraient pas présenter de publicité sur la base d’un profilage, tel qu’il est défini à l’article 4, point 4), du règlement (UE) 2016/679, en utilisant les catégories particulières de données à caractère personnel visées à l’article 9, paragraphe 1, dudit règlement, y compris en utilisant des catégories de profilage fondées sur ces catégories particulières. Cette interdiction est sans préjudice des obligations applicables aux fournisseurs de plateformes en ligne ou à tout autre fournisseur de services ou annonceur participant à la diffusion des publicités en vertu du droit de l’Union en matière de protection des données à caractère personnel.

(70)

La manière dont les informations sont hiérarchisées et présentées sur l’interface en ligne d’une plateforme en ligne afin de faciliter et d’optimiser l’accès aux informations pour les destinataires du service occupe une place essentielle dans les activités de la plateforme. Cela consiste, par exemple, à suggérer, classer et hiérarchiser les informations de manière algorithmique, en les distinguant par le texte ou par d’autres représentations visuelles, ou en organisant de toute autre manière les informations fournies par les destinataires. Ces systèmes

de recommandation peuvent avoir une incidence significative sur la capacité des destinataires à récupérer les informations en ligne et à interagir avec elles, y compris pour faciliter la recherche d'informations pertinentes pour les destinataires du service et contribuer à améliorer l'expérience utilisateur. Ils jouent également un rôle important dans l'amplification de certains messages, la diffusion virale de l'information et la stimulation du comportement en ligne. Par conséquent, les plateformes en ligne devraient veiller en permanence à ce que les destinataires de leur service soient correctement informés de la manière dont les systèmes de recommandation ont un effet sur la manière dont l'information est affichée et peuvent influencer la manière dont les informations leur sont présentées. Elles devraient présenter clairement les paramètres de ces systèmes de recommandation d'une manière facilement compréhensible afin que les destinataires du service comprennent comment l'information est hiérarchisée à leur intention. Ces paramètres devraient inclure au moins les critères les plus importants utilisés pour déterminer les informations suggérées au destinataire du service et les raisons de leur importance respective, y compris lorsque les informations sont hiérarchisées sur la base du profilage et du comportement en ligne des destinataires.

(71)

La protection des mineurs est un objectif stratégique important de l'Union. Une plateforme en ligne peut être considérée comme accessible aux mineurs lorsque ses conditions générales permettent aux mineurs d'utiliser le service, lorsque son service s'adresse aux mineurs ou est utilisé de manière prédominante par des mineurs, ou lorsque le fournisseur sait par ailleurs que certains des destinataires de son service sont des mineurs, par exemple parce qu'il traite déjà des données à caractère personnel des destinataires de son service révélant leur âge à d'autres fins. Les fournisseurs de plateformes en ligne utilisées par des mineurs devraient prendre des mesures appropriées et proportionnées pour protéger les mineurs, par exemple en concevant leurs interfaces en ligne ou des parties de celles-ci avec le plus haut niveau de protection de la vie privée, de sécurité et de sûreté des mineurs par défaut, s'il y a lieu, ou en adoptant des normes de protection des mineurs, ou en participant à des codes de conduite pour la protection des mineurs. Ils devraient tenir compte des bonnes pratiques et des orientations disponibles, telles que celles fournies dans la communication de la Commission intitulée "Une décennie numérique pour les enfants et les jeunes: la nouvelle stratégie européenne pour un internet mieux adapté aux enfants". Les fournisseurs de plateformes en ligne ne devraient pas présenter de publicité qui repose sur le profilage utilisant des données à caractère personnel concernant le destinataire du service dès lors qu'ils savent avec une certitude raisonnable que le destinataire du service est un mineur. Conformément au règlement (UE) 2016/679, et notamment au principe de minimisation des données prévu à l'article 5, paragraphe 1, point c), dudit règlement, cette interdiction ne devrait pas conduire le fournisseur de la plateforme en ligne à conserver, à acquérir ou à traiter davantage de données à caractère personnel qu'il n'en détient déjà afin d'évaluer si le destinataire du service est un mineur. Par conséquent, cette obligation ne devrait pas inciter les fournisseurs de plateformes en ligne à recueillir l'âge du destinataire du service avant l'utilisation de ces plateformes. Ceci devrait s'appliquer sans préjudice du droit de l'Union en matière de protection des données à caractère personnel.

(72)

Afin de contribuer à un environnement en ligne sûr, fiable et transparent pour les consommateurs, ainsi que pour les autres parties intéressées telles que les professionnels concurrents et les titulaires de droits de propriété intellectuelle, et de dissuader les professionnels de vendre des produits ou des services en violation des règles applicables, il

convient que les plateformes en ligne permettant aux consommateurs de conclure des contrats à distance avec des professionnels garantissent la traçabilité de ces derniers. Le professionnel devrait donc être tenu de fournir certaines informations essentielles aux fournisseurs de plateformes en ligne permettant aux consommateurs de conclure des contrats à distance avec des professionnels, notamment aux fins de la promotion de messages concernant des produits ou l'offre de produits. Cette exigence devrait également être applicable aux professionnels qui font la promotion de messages concernant des produits ou des services pour le compte de marques, sur la base d'accords sous-jacents. Il convient que ces fournisseurs de plateformes en ligne conservent toutes les informations de manière sécurisée pendant la durée de leur relation contractuelle avec le professionnel et six mois après la fin de celle-ci, afin que toute réclamation à l'encontre du professionnel puisse être déposée ou que les injonctions le concernant puissent être respectées.

Cette obligation est nécessaire et proportionnée, de manière à ce que les autorités publiques et les parties privées ayant un intérêt légitime puissent avoir accès aux informations, dans le respect du droit applicable, y compris en matière de protection des données à caractère personnel, notamment au moyen des injonctions de fournir des informations prévues par le présent règlement. Cette obligation ne modifie en rien les éventuelles obligations de préserver des contenus déterminés pendant des périodes plus longues, sur la base d'autres dispositions du droit de l'Union ou d'autres dispositions du droit national conforme au droit de l'Union. Sans préjudice de la définition figurant dans le présent règlement, tout professionnel, qu'il s'agisse d'une personne physique ou morale, identifié sur la base de l'article 6 bis, paragraphe 1, point b), de la directive 2011/83/UE et de l'article 7, paragraphe 4, point f), de la directive 2005/29/CE devrait être traçable lorsqu'il propose un produit ou un service par l'intermédiaire d'une plateforme en ligne. La directive 2000/31/CE impose à tous les prestataires de services de la société de l'information de rendre possible un accès facile, direct et permanent, pour les destinataires du service et pour les autorités compétentes, à certaines informations permettant l'identification de tous les prestataires. Les exigences en matière de traçabilité applicables aux fournisseurs de plateformes en ligne permettant aux consommateurs de conclure des contrats à distance avec des professionnels, énoncées dans le présent règlement, n'affectent pas l'application de la directive (UE) 2021/514 du Conseil (30), qui poursuit d'autres objectifs légitimes d'intérêt public.

(73)

Pour que cette obligation soit appliquée de manière efficace et adéquate, sans imposer de contraintes disproportionnées, les fournisseurs de plateformes en ligne permettant aux consommateurs de conclure des contrats à distance avec des professionnels devraient déployer tous leurs efforts en vue d'évaluer la fiabilité des informations fournies par les professionnels concernés, notamment en utilisant des bases de données en ligne et des interfaces en ligne officielles librement accessibles, telles que les registres du commerce nationaux et le système d'échange d'informations sur la TVA, ou demander aux professionnels concernés de fournir des documents justificatifs fiables, telles que des copies de documents d'identité, des relevés de comptes de paiement certifiés, des certificats d'entreprise et des certificats d'immatriculation au registre du commerce. Ils peuvent également utiliser d'autres sources, disponibles pour une utilisation à distance, qui présentent un degré équivalent de fiabilité aux fins du respect de cette obligation. Toutefois, les fournisseurs de plateformes en ligne concernés ne devraient pas être tenus de se livrer à des recherches de faits en ligne excessives ou coûteuses ou de procéder à des vérifications disproportionnées sur place. Les fournisseurs qui ont déployé tous les efforts requis par le présent règlement ne devraient pas non plus être

réputés garantir la fiabilité des informations à l'égard du consommateur ou d'autres parties intéressées.

(74)

Il convient également que les fournisseurs de plateformes en ligne permettant aux consommateurs de conclure des contrats à distance avec des professionnels conçoivent et organisent leur interface en ligne de manière à permettre aux professionnels de respecter les obligations qui leur incombent en vertu du droit de l'Union applicable, en particulier les exigences énoncées aux articles 6 et 8 de la directive 2011/83/UE, à l'article 7 de la directive 2005/29/CE, aux articles 5 et 6 de la directive 2000/31/CE et à l'article 3 de la directive 98/6/CE du Parlement européen et du Conseil (31). À cette fin, les fournisseurs de plateformes en ligne concernés devraient déployer tous leurs efforts en vue d'examiner si les professionnels utilisant leurs services ont téléchargé des informations complètes sur leurs interfaces en ligne, conformément au droit de l'Union applicable pertinent. Les fournisseurs de plateformes en ligne devraient veiller à ce que les produits ou services ne soient pas proposés tant que ces informations ne sont pas complètes. Cela ne devrait pas équivaloir pour les fournisseurs de plateformes en ligne concernés à une obligation générale de surveillance des produits ou des services proposés par les professionnels par l'intermédiaire de leurs services ni à une obligation générale de recherche des faits, notamment aux fins de vérifier l'exactitude des informations fournies par les professionnels. Les interfaces en ligne devraient être faciles d'accès et faciles à utiliser pour les professionnels et les consommateurs. En outre, une fois qu'ils ont autorisé le professionnel à proposer un produit ou service, les fournisseurs de plateformes en ligne concernés s'efforcent, dans la mesure du raisonnable, de contrôler aléatoirement si les produits ou services proposés ont été signalés comme étant illégaux dans des bases de données en ligne ou des interfaces en ligne officielles, librement accessibles et lisibles par une machine, disponibles dans un État membre ou dans l'Union. La Commission devrait également encourager la traçabilité des produits au moyen de solutions technologiques telles que des codes à réponse rapide signés numériquement (ou "codes QR") ou des jetons non fongibles. La Commission devrait promouvoir l'élaboration de normes et, en l'absence de ces dernières, l'élaboration de solutions fondées sur le marché qui peuvent être acceptables pour les parties concernées.

(75)

Compte tenu du rôle important que jouent les très grandes plateformes en ligne, en raison de leur portée, exprimée notamment en nombre de destinataires du service, s'agissant de faciliter le débat public, les transactions économiques, et la diffusion au public d'informations, d'opinions et d'idées, et d'influencer la manière dont les destinataires obtiennent et communiquent des informations en ligne, il est nécessaire d'imposer aux fournisseurs de ces plateformes des obligations spécifiques venant s'ajouter aux obligations applicables à toutes les plateformes en ligne. En raison de leur rôle essentiel dans la localisation et la possibilité de récupérer des informations en ligne, il est également nécessaire d'imposer ces obligations, dans la mesure où elles sont applicables, aux fournisseurs de très grands moteurs de recherche en ligne. Ces obligations supplémentaires imposées aux fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne sont nécessaires pour répondre aux considérations de politique publique, dans la mesure où il n'existe pas d'autres mesures moins restrictives qui permettraient d'atteindre effectivement le même résultat.

(76)

Les très grandes plateformes en ligne et les très grands moteurs de recherche en ligne peuvent engendrer des risques pour la société, qui diffèrent, par leur ampleur et leur incidence, de ceux qui sont imputables aux plateformes de plus petite taille. Les fournisseurs de ces très grandes plateformes en ligne et de ces très grands moteurs de recherche en ligne devraient donc être soumis aux normes les plus strictes en matière d'obligations de diligence, proportionnellement à leurs effets sur la société. Lorsque le nombre de destinataires actifs d'une plateforme en ligne ou de destinataires actifs d'un moteur de recherche en ligne, calculé comme une moyenne sur une période de six mois, représente une part significative de la population de l'Union, les risques systémiques présentés par la plateforme en ligne ou le moteur de recherche en ligne peuvent produire des effets disproportionnés dans l'Union. On peut considérer qu'une portée significative est atteinte lorsque ce nombre dépasse un seuil opérationnel fixé à 45 millions, c'est-à-dire un nombre équivalent à 10 % de la population de l'Union. Ce seuil opérationnel devrait être maintenu à jour et, par conséquent, la Commission devrait être habilitée à compléter les dispositions du présent règlement en adoptant des actes délégués, si nécessaire.

(77)

Afin de déterminer la portée d'une plateforme en ligne ou d'un moteur de recherche en ligne donné, il est nécessaire d'établir le nombre moyen de destinataires actifs de chaque service individuellement. En conséquence, le nombre moyen de destinataires mensuels actifs d'une plateforme en ligne devrait refléter tous les destinataires utilisant effectivement le service au moins une fois au cours d'une période donnée, en étant exposés à des informations diffusées sur l'interface en ligne de la plateforme en ligne, par exemple en les regardant ou en les écoutant, ou en fournissant des informations, comme les professionnels sur des plateformes en ligne permettant aux consommateurs de conclure des contrats à distance avec des professionnels.

Aux fins du présent règlement, l'utilisation active ne se limite pas à interagir avec des informations en cliquant dessus, en les commentant, en les affichant en lien, en les partageant, en procédant à des achats ou en effectuant des transactions sur une plateforme en ligne. Par conséquent, la notion de destinataire actif du service ne coïncide pas nécessairement avec celle d'utilisateur inscrit d'un service. En ce qui concerne les moteurs de recherche en ligne, la notion de destinataires actifs du service devrait comprendre ceux qui consultent les informations sur leur interface en ligne, mais pas, par exemple, les propriétaires des sites internet indexés par un moteur de recherche en ligne, car ils n'utilisent pas activement le service. Le nombre de destinataires actifs d'un service devrait inclure tous les destinataires uniques du service qui utilisent activement ce service spécifique. À cet effet, un destinataire du service qui utilise différentes interfaces en ligne, telles que des sites internet ou des applications, y compris lorsque les services sont accessibles au moyen de différents localisateurs uniformes de ressources (URL) ou noms de domaine, ne devrait, dans la mesure du possible, être comptabilisé qu'une seule fois. Toutefois, la notion de destinataire actif du service ne devrait pas inclure l'utilisation accessoire du service par les destinataires d'autres fournisseurs de services intermédiaires qui mettent indirectement à disposition des informations hébergées par le fournisseur de plateformes en ligne via la fourniture d'un lien ou l'indexation par un fournisseur de moteur de recherche en ligne. En outre, le présent règlement n'impose pas aux fournisseurs de plateformes en ligne ou de moteurs de recherche en ligne d'effectuer un pistage spécifique des personnes en ligne. Lorsque ces fournisseurs sont en mesure d'exclure du décompte les utilisateurs automatisés tels que les robots ou les

récupérateurs d'informations ("scrapers") sans autre traitement des données à caractère personnel ni pistage, ils peuvent le faire. La détermination du nombre de destinataires actifs du service pouvant être influencée par les évolutions du marché et les évolutions techniques, la Commission devrait être habilitée à compléter les dispositions du présent règlement en adoptant des actes délégués établissant la méthode permettant de déterminer les destinataires actifs d'une plateforme en ligne ou d'un moteur de recherche en ligne, si nécessaire, en tenant compte de la nature du service et de la manière dont les destinataires du service interagissent avec celui-ci.

(78)

Compte tenu des effets de réseau qui caractérisent l'économie des plateformes, la base d'utilisateurs d'une plateforme en ligne ou d'un moteur de recherche en ligne peut rapidement s'accroître et atteindre la dimension d'une très grande plateforme en ligne ou d'un très grand moteur de recherche en ligne, avec une incidence correspondante sur le marché intérieur. Cela peut se produire si une croissance exponentielle est enregistrée sur de courtes périodes, ou si l'importance de la présence et du chiffre d'affaires mondiaux de la plateforme en ligne ou du moteur de recherche en ligne lui permet d'exploiter pleinement les effets de réseau et les économies d'échelle et de gamme. Un chiffre d'affaires annuel important ou une capitalisation boursière annuelle élevée peuvent notamment être des indices de la capacité d'évolution rapide de l'audience. Dans de tels cas, le coordinateur pour les services numériques de l'État membre d'établissement ou la Commission devraient pouvoir demander au fournisseur de la plateforme en ligne ou du moteur de recherche en ligne de soumettre plus fréquemment des rapports sur le nombre de destinataires actifs du service afin de pouvoir déterminer à temps le moment à partir duquel cette plateforme ou ce moteur de recherche devrait être désigné comme une très grande plateforme en ligne ou un très grand moteur de recherche en ligne, respectivement, aux fins du présent règlement.

(79)

Les très grandes plateformes en ligne et les très grands moteurs de recherche en ligne peuvent être utilisés d'une manière qui a une influence considérable sur la sécurité en ligne, sur la formation de l'opinion publique et du discours, ainsi que sur le commerce en ligne. La façon dont ils conçoivent leurs services est généralement optimisée au bénéfice de leurs modèles économiques souvent axés sur la publicité et peut susciter des préoccupations sociétales. Une réglementation et une exécution efficaces sont nécessaires pour déterminer et atténuer efficacement les risques et le préjudice sociétal et économique potentiels. En vertu du présent règlement, les fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne devraient donc évaluer les risques systémiques découlant de la conception, du fonctionnement et de l'utilisation de leurs services, ainsi que des abus potentiels par les destinataires du service, et devraient prendre des mesures d'atténuation appropriées, dans le respect des droits fondamentaux. Pour déterminer l'ampleur des effets et impact négatifs potentiels, les fournisseurs devraient examiner la gravité de l'impact potentiel et la probabilité de tous ces risques systémiques. Par exemple, ils pourraient évaluer si l'impact négatif potentiel peut toucher un grand nombre de personnes, déterminer son éventuelle irréversibilité ou apprécier à quel point il est difficile de remédier au problème et de revenir à la situation antérieure à l'impact potentiel.

(80)

Quatre catégories de risques systémiques devraient être évaluées de manière approfondie par les fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne. Dans la première catégorie figurent les risques associés à la diffusion de contenus illicites, tels que la diffusion de matériel pédopornographique, de discours haineux illégaux ou d'autres types d'usage abusif de leurs services dans le cadre d'infractions pénales, et la poursuite d'activités illégales, telles que la vente de produits ou de services interdits par le droit de l'Union ou le droit national, y compris des produits dangereux ou de contrefaçon, ou des animaux commercialisés illégalement. Par exemple, cette diffusion ou ces activités peuvent constituer un risque systémique important lorsque l'accès à des contenus illicites peut se propager rapidement et largement grâce à des comptes d'une portée particulièrement large ou à d'autres moyens d'amplification. Les fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne devraient évaluer le risque de diffusion de contenus illicites, que l'information soit ou non également incompatible avec leurs conditions générales. Cette évaluation est sans préjudice de la responsabilité personnelle du destinataire du service de très grandes plateformes en ligne ou des propriétaires de sites internet indexés par de très grands moteurs de recherche en ligne du fait de l'éventuelle illégalité de leur activité au regard du droit applicable.

(81)

La deuxième catégorie concerne l'incidence réelle ou prévisible du service sur l'exercice des droits fondamentaux, tels qu'ils sont protégés par la Charte, ce qui comprend, sans s'y limiter, la dignité humaine, la liberté d'expression et d'information, dont la liberté et le pluralisme des médias, le droit à la vie privée, la protection des données, le droit à la non-discrimination, les droits de l'enfant et la protection des consommateurs. De tels risques peuvent découler, par exemple, de la conception des systèmes algorithmiques utilisés par la très grande plateforme en ligne ou par le très grand moteur de recherche en ligne, ou de l'usage abusif de leur service par la soumission de notifications abusives ou d'autres méthodes visant à réduire au silence ou à entraver la concurrence. Lorsqu'ils évaluent les risques pour les droits de l'enfant, les fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne devraient examiner par exemple à quel point la conception et le fonctionnement du service sont faciles à comprendre pour les mineurs, ainsi que la manière dont ces derniers peuvent être exposés, par le biais de leur service, à des contenus pouvant nuire à leur santé ainsi qu'à leur épanouissement physique, mental et moral. Ces risques peuvent résulter, par exemple, de la conception des interfaces en ligne qui exploitent intentionnellement ou non les faiblesses et l'inexpérience des mineurs ou qui peuvent entraîner un comportement de dépendance.

(82)

La troisième catégorie de risques concerne les effets négatifs réels ou prévisibles sur les processus démocratiques, le discours civique et les processus électoraux, ainsi que sur la sécurité publique.

(83)

Une quatrième catégorie de risques découle de préoccupations similaires relatives à la conception, au fonctionnement ou à l'utilisation, y compris par manipulation, de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne ayant un effet négatif réel ou prévisible sur la protection de la santé publique et des mineurs, ainsi que des conséquences

négatives graves sur le bien-être physique et mental d'une personne, ou sur la violence à caractère sexiste. Ces risques peuvent également résulter de campagnes de désinformation coordonnées liées à la santé publique ou de la conception d'interfaces en ligne susceptibles de stimuler les dépendances comportementales des destinataires du service.

(84)

Lors de l'évaluation de ces risques systémiques, les fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne devraient se concentrer sur les systèmes ou autres éléments susceptibles de contribuer aux risques, y compris tous les systèmes algorithmiques qui peuvent être concernés, en particulier leurs systèmes de recommandation et leurs systèmes publicitaires, en étant attentifs aux pratiques connexes en matière de collecte et d'utilisation des données. Ils devraient également évaluer si leurs conditions générales et la mise en application de ces dernières sont appropriées, ainsi que leurs processus de modération des contenus, leurs outils techniques et les ressources affectées. Lors de l'évaluation des risques systémiques recensés dans le présent règlement, ces fournisseurs devraient également se concentrer sur les informations qui ne sont pas illicites mais alimentent les risques systémiques recensés dans le présent règlement. Ces fournisseurs devraient donc accorder une attention particulière à la manière dont leurs services sont utilisés pour diffuser ou amplifier des contenus trompeurs ou mensongers, et notamment à la désinformation. Lorsque l'amplification algorithmique des informations contribue aux risques systémiques, ces fournisseurs devraient en tenir dûment compte dans leurs évaluations des risques. Lorsque les risques sont localisés ou qu'il existe des différences linguistiques, il y a lieu que ces fournisseurs en rendent compte également dans leurs évaluations des risques. Les fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne devraient, en particulier, examiner la manière dont la conception et le fonctionnement de leurs services, ainsi que l'utilisation et la manipulation intentionnelles et, souvent, coordonnées de leurs services, ou la violation systémique de leurs conditions d'utilisation, contribuent à ces risques. Ces risques peuvent résulter, par exemple, de l'utilisation non authentique du service, telle que la création de faux comptes, l'utilisation de robots ou l'utilisation trompeuse d'un service, et d'autres comportements automatisés ou partiellement automatisés, susceptibles de conduire à la diffusion rapide et généralisée au public d'informations qui constituent un contenu illicite ou qui sont incompatibles avec les conditions générales d'une plateforme en ligne ou d'un moteur de recherche en ligne et qui contribuent à des campagnes de désinformation.

(85)

Afin que les évaluations des risques ultérieures puissent s'appuyer les unes sur les autres et montrer l'évolution des risques recensés, ainsi que pour faciliter les enquêtes et les mesures d'exécution, les fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne devraient conserver tous les documents justificatifs relatifs aux évaluations des risques qu'ils ont effectuées, tels que les informations relatives à leur préparation, les données sous-jacentes et les données sur les essais de leurs systèmes algorithmiques.

(86)

Les fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne devraient déployer les moyens nécessaires pour atténuer avec diligence les risques systémiques recensés dans les évaluations des risques, dans le respect des droits

fondamentaux. Toute mesure adoptée devrait respecter les exigences de diligence du présent règlement, être raisonnable et atténuer efficacement les risques systémiques spécifiques recensés. Ces mesures devraient être proportionnées à la capacité économique du fournisseur de la très grande plateforme en ligne ou du très grand moteur de recherche en ligne et à la nécessité d'éviter des restrictions inutiles à l'utilisation de leur service, compte devant dûment être tenu des effets négatifs potentiels sur les droits fondamentaux. Ces fournisseurs devraient accorder une attention particulière aux répercussions sur la liberté d'expression.

(87)

Dans le cadre de ces mesures d'atténuation, les fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne devraient envisager, par exemple, d'adapter toute conception, toute caractéristique ou tout fonctionnement nécessaires de leur service, comme la conception des interfaces en ligne. Ils devraient adapter et appliquer leurs conditions générales, si nécessaire et conformément aux règles du présent règlement relatives aux conditions générales. D'autres mesures appropriées pourraient comprendre l'adaptation de leurs systèmes de modération des contenus et de leurs processus internes ou l'adaptation de leurs processus décisionnels et de leurs ressources, notamment le personnel chargé de la modération des contenus, leur formation et leur expertise locale. Cela concerne en particulier la rapidité et la qualité du traitement des notifications. À cet égard, par exemple, le code de conduite pour la lutte contre les discours haineux illégaux en ligne de 2016 fixe un critère de référence pour le traitement des notifications valides en vue du retrait des discours haineux illégaux en moins de 24 heures. Les fournisseurs de très grandes plateformes en ligne, en particulier celles qui sont principalement utilisées pour la diffusion au public de contenus pornographiques, devraient s'acquitter avec diligence de toutes les obligations qui leur incombent en vertu du présent règlement en ce qui concerne les contenus illicites constituant de la cyberviolence, en particulier les contenus pornographiques illicites, en veillant plus particulièrement à ce que les victimes puissent effectivement exercer leurs droits en lien avec des contenus constituant un partage non consensuel de contenus intimes ou de matériel manipulé, et ce en traitant rapidement les notifications et en procédant au retrait des contenus en question sans retard injustifié. D'autres types de contenus illicites peuvent nécessiter des délais plus longs ou plus courts pour le traitement des notifications, en fonction des faits, des circonstances et des types de contenus illicites en cause. Ces fournisseurs peuvent également mettre en place une coopération ou renforcer une coopération existante avec des signaleurs de confiance et organiser des sessions de formation et des échanges avec des organisations de signaleurs de confiance.

(88)

Les fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne devraient également faire preuve de diligence dans les mesures qu'ils prennent pour tester et, si nécessaire, adapter leurs systèmes algorithmiques, en particulier leurs systèmes de recommandation. Ils peuvent devoir atténuer les effets négatifs de recommandations personnalisées et à corriger les critères utilisés dans leurs recommandations. Les systèmes publicitaires utilisés par les fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne peuvent également être un catalyseur pour les risques systémiques. Ces fournisseurs devraient envisager de prendre des mesures correctives consistant par exemple à mettre fin aux revenus publicitaires pour des informations déterminées ou d'autres mesures, telles que les mesures visant à accroître la visibilité des sources d'information faisant autorité, ou à adapter leurs systèmes publicitaires davantage sur

le plan structurel. Les fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne peuvent devoir renforcer leurs processus internes ou la surveillance d'une ou plusieurs de leurs activités, notamment en ce qui concerne la détection des risques systémiques, et procéder à des évaluations des risques plus fréquentes ou plus ciblées liées aux nouvelles fonctionnalités. En particulier, lorsque les risques sont communs à différentes plateformes en ligne ou moteurs de recherche en ligne, ils devraient coopérer avec d'autres fournisseurs de services, notamment en mettant en chantier des codes de conduite ou d'autres mesures d'autorégulation ou en adhérant à des codes de conduite ou à de telles mesures existants. Ils devraient également envisager des actions de sensibilisation, en particulier lorsque les risques sont liés à des campagnes de désinformation.

(89)

Les fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne devraient tenir compte de l'intérêt supérieur des mineurs lorsqu'ils prennent des mesures telles que l'adaptation de la conception de leur service et de leur interface en ligne, plus particulièrement lorsque leurs services s'adressent aux mineurs ou sont utilisés de manière prédominante par ceux-ci. Ils devraient veiller à ce que leurs services soient organisés de manière à permettre aux mineurs d'accéder facilement aux mécanismes prévus par le présent règlement, le cas échéant, y compris aux mécanismes de notification et d'action et aux mécanismes de réclamation. En outre, ils devraient prendre des mesures pour protéger les mineurs contre les contenus susceptibles de nuire à leur épanouissement physique, mental ou moral et fournir des outils permettant un accès conditionnel à ces informations. Lorsqu'ils choisissent les mesures d'atténuation appropriées, les fournisseurs peuvent prendre en compte, le cas échéant, les bonnes pratiques du secteur, y compris celles établies au moyen d'une coopération en matière d'autorégulation, telles que les codes de conduite, et devraient tenir compte des lignes directrices de la Commission.

(90)

Les fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne devraient veiller à ce que leur approche de l'évaluation et de l'atténuation des risques soit fondée sur les meilleures informations et connaissances scientifiques disponibles et à mettre à l'essai leurs hypothèses auprès des groupes les plus affectés par les risques et les mesures prises. Il convient à cette fin que les fournisseurs procèdent, le cas échéant, à leurs évaluations des risques et conçoivent leurs mesures d'atténuation des risques avec la participation de représentants des destinataires du service, de représentants de groupes potentiellement affectés par leurs services, d'experts indépendants et d'organisations de la société civile. Ils devraient s'efforcer d'intégrer ces consultations, comprenant, le cas échéant, des enquêtes, des groupes de réflexion, des tables rondes et d'autres méthodes de consultation et de conception, dans leurs méthodes d'évaluation des risques et de conception des mesures d'atténuation. Lors de l'évaluation du caractère raisonnable, proportionné et efficace d'une mesure, il convient d'accorder une attention particulière au droit à la liberté d'expression.

(91)

En temps de crise, les fournisseurs de très grandes plateformes en ligne pourraient devoir prendre certaines mesures spécifiques d'urgence, en plus des mesures qu'ils prendraient compte tenu de leurs autres obligations au titre du présent règlement. À cet égard, il y a lieu de conclure à une crise lorsque des circonstances extraordinaires peuvent entraîner une

menace grave pour la sécurité publique ou la santé publique dans l'Union ou dans des parties importantes de l'Union. Ces crises pourraient résulter de conflits armés ou d'actes de terrorisme, existants ou nouveaux, de catastrophes naturelles telles que des tremblements de terre et des ouragans, ainsi que de pandémies et d'autres menaces transfrontières graves pour la santé publique. La Commission devrait être en mesure d'exiger, sur recommandation du comité européen pour les services numériques (ci-après dénommé "comité"), que les fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne initient d'urgence une réaction aux crises. Les mesures que ces fournisseurs peuvent déterminer et envisager d'appliquer comprennent, par exemple, l'adaptation des processus de modération des contenus et l'augmentation des ressources consacrées à la modération des contenus, l'adaptation des conditions générales, des systèmes algorithmiques et des systèmes publicitaires concernés, l'intensification de la coopération avec les signaleurs de confiance, la prise de mesures de sensibilisation, la promotion d'informations fiables et l'adaptation de la conception de leurs interfaces en ligne. Il convient de prévoir les exigences nécessaires pour garantir que ces mesures sont prises dans un délai très court et que le mécanisme de réaction aux crises n'est utilisé que lorsque, et dans la mesure où, cela est strictement nécessaire et que toute mesure prise au titre de ce mécanisme est efficace et proportionnée, compte étant dûment tenu des droits et des intérêts légitimes de toutes les parties concernées. Le recours au mécanisme devrait être sans préjudice des autres dispositions du présent règlement, telles que celles relatives à l'évaluation des risques et aux mesures d'atténuation des risques et à leur exécution, ainsi que celles relatives aux protocoles de crise.

(92)

Compte tenu de la nécessité de garantir une vérification par des experts indépendants, les fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne devraient être tenus de rendre des comptes, dans le cadre d'un audit indépendant, en ce qui concerne leur respect des obligations prévues dans le présent règlement et, le cas échéant, de tout engagement complémentaire pris en vertu de codes de conduite et de protocoles de crise. Afin de garantir que les audits sont réalisés de manière efficace, efficiente et en temps utile, les fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne devraient fournir la coopération et l'assistance nécessaires aux organisations effectuant les audits, y compris en donnant à l'auditeur l'accès à l'ensemble des données pertinentes et aux locaux nécessaires pour effectuer correctement l'audit, y compris, le cas échéant, aux données relatives aux systèmes algorithmiques, et en répondant aux questions orales ou écrites. Les auditeurs devraient également pouvoir utiliser d'autres sources d'informations objectives, y compris des études réalisées par des chercheurs agréés. Les fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne ne sauraient entraver la réalisation de l'audit. Les audits devraient être réalisés conformément aux bonnes pratiques du secteur et en respectant un niveau élevé d'éthique professionnelle et d'objectivité, en tenant dûment compte, le cas échéant, des normes d'audit et des codes de bonnes pratiques. Les auditeurs devraient garantir la confidentialité, la sécurité et l'intégrité des informations, telles que les secrets d'affaires, qu'ils obtiennent dans l'accomplissement de leurs tâches. Cette garantie ne devrait pas être un moyen de contourner l'applicabilité des obligations en matière d'audit prévues par le présent règlement. Les auditeurs devraient disposer de l'expertise nécessaire dans le domaine de la gestion des risques et des compétences techniques pour vérifier les algorithmes. Ils devraient être indépendants, afin de pouvoir accomplir leurs tâches de manière adéquate et fiable. Ils devraient respecter les exigences fondamentales en matière d'indépendance en ce qui concerne les services extérieurs à la mission d'audit interdits, la rotation des cabinets d'audit

et les honoraires non conditionnels. Si leur indépendance et leurs compétences techniques ne sont pas incontestables, ils devraient démissionner ou s'abstenir d'effectuer la mission d'audit.

(93)

Le rapport d'audit devrait être étayé, afin de rendre compte de manière judicieuse des activités entreprises et des conclusions auxquelles elles ont abouti. Il devrait contribuer à nourrir la réflexion sur les mesures prises par les fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne pour se conformer à leurs obligations au titre du présent règlement et, le cas échéant, suggérer des améliorations de ces mesures. Le rapport d'audit devrait être transmis après réception au coordinateur pour les services numériques de l'État membre d'établissement, à la Commission et au comité. Les fournisseurs devraient également transmettre sans retard injustifié, dès leur achèvement, chacun des rapports sur l'évaluation des risques et les mesures d'atténuation, ainsi que le rapport de mise en œuvre des recommandations de l'audit du fournisseur de la très grande plateforme en ligne ou du très grand moteur de recherche en ligne, dans lequel ces derniers indiquent comment ils ont donné suite aux recommandations de l'audit. Le rapport d'audit devrait comprendre un avis d'audit fondé sur les conclusions tirées des éléments probants recueillis dans le cadre de l'audit. Un "avis positif" devrait être rendu lorsque tous les éléments probants montrent que le fournisseur de la très grande plateforme en ligne ou du très grand moteur de recherche en ligne respecte les obligations prévues par le présent règlement ou, le cas échéant, les éventuels engagements qu'il ou elle a pris en vertu d'un code de conduite ou d'un protocole de crise, notamment en déterminant, en évaluant et en atténuant les risques systémiques présentés par son système et ses services. L'"avis positif" devrait être assorti de commentaires lorsque l'auditeur souhaite inclure des observations qui n'ont pas d'incidence importante sur le résultat de l'audit. Un "avis négatif" devrait être émis lorsque l'auditeur estime que le fournisseur de la très grande plateforme en ligne ou du très grand moteur de recherche en ligne ne respecte pas le présent règlement ou les engagements pris. Lorsqu'un avis d'audit n'a pu aboutir à aucune conclusion sur des éléments spécifiques relevant du champ de l'audit, une explication des raisons du défaut de conclusions devrait être intégrée dans l'avis d'audit. Le cas échéant, le rapport devrait comprendre une description des éléments spécifiques qui n'ont pas pu être audités, et une explication de la raison pour laquelle ils n'ont pas pu l'être.

(94)

Les obligations en matière d'évaluation et d'atténuation des risques devraient entraîner, au cas par cas, la nécessité pour les fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne d'évaluer et, si nécessaire, d'ajuster la conception de leurs systèmes de recommandation, par exemple en prenant des mesures pour prévenir et réduire le plus possible les biais qui conduisent à la discrimination de personnes en situation de vulnérabilité, en particulier lorsque cet ajustement est conforme au droit en matière de protection des données et lorsque les informations sont personnalisées en fonction de catégories particulières de données à caractère personnel visées à l'article 9 du règlement (UE) 2016/679. En outre, et en complément des obligations de transparence applicables aux plateformes en ligne en ce qui concerne leurs systèmes de recommandation, les fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne devraient veiller systématiquement à ce que les destinataires de leur service bénéficient d'autres options qui ne sont pas fondées sur le profilage, au sens du règlement (UE) 2016/679, pour les principaux paramètres de leurs systèmes de recommandation. Ces choix devraient être

directement accessibles à partir de l’interface en ligne où les recommandations sont présentées.

(95)

Les systèmes publicitaires utilisés par les très grandes plateformes en ligne et les très grands moteurs de recherche en ligne présentent des risques particuliers et nécessitent un contrôle public et réglementaire plus poussé en raison de leur envergure et de leur capacité à cibler et à atteindre les destinataires du service en fonction de leur comportement à l’intérieur et à l’extérieur de l’interface en ligne de cette plateforme ou de ce moteur de recherche. Les très grandes plateformes en ligne ou les très grands moteurs de recherche en ligne devraient garantir l’accès du public aux registres des publicités présentées sur leurs interfaces en ligne afin de faciliter la surveillance et les recherches relatifs aux risques émergents engendrés par la diffusion de publicités en ligne, par exemple en ce qui concerne les publicités illégales ou les techniques de manipulation et de désinformation ayant un effet négatif réel et prévisible sur la santé publique, la sécurité publique, le discours civique, la participation politique et l’égalité. Les registres devraient inclure le contenu des publicités, y compris le nom du produit, du service ou de la marque et l’objet de la publicité, et les données connexes concernant l’annonceur et, si elle est différente, la personne physique ou morale qui a financé la publicité, et la diffusion de la publicité, en particulier lorsqu’il s’agit de publicité ciblée. Ces informations devraient comprendre des informations relatives tant aux critères de ciblage qu’aux critères de diffusion, en particulier lorsque les publicités sont diffusées auprès de personnes en situation de vulnérabilité, comme les mineurs.

(96)

Afin de surveiller et d’évaluer de manière appropriée le respect par les très grandes plateformes en ligne et les très grands moteurs de recherche en ligne des obligations prévues par le présent règlement, le coordinateur pour les services numériques de l’État membre d’établissement ou la Commission peut exiger l’accès à des données spécifiques ou la communication de celles-ci, y compris les données relatives aux algorithmes. Une telle exigence peut porter, par exemple, sur les données nécessaires pour évaluer les risques et les éventuels préjudices causés par les systèmes de la très grande plateforme en ligne ou du très grand moteur de recherche en ligne, les données concernant l’exactitude, le fonctionnement et les tests des systèmes algorithmiques de modération des contenus, des systèmes de recommandation ou des systèmes de publicité, y compris, le cas échéant, les données et algorithmes d’entraînement, ou encore les données concernant les processus et les résultats de la modération des contenus ou des systèmes internes de traitement des réclamations au sens du présent règlement. Ces demandes d’accès aux données ne devraient pas comprendre les demandes de production d’informations spécifiques sur des destinataires individuels du service visant à déterminer si ces destinataires respectent d’autres dispositions applicables du droit de l’Union ou du droit national. Les enquêtes menées par des chercheurs sur l’évolution et la gravité des risques systémiques en ligne sont particulièrement importantes pour corriger les asymétries d’information et établir un système résilient d’atténuation des risques, informer les fournisseurs des plateformes en ligne, les fournisseurs des moteurs de recherche en ligne, les coordinateurs pour les services numériques, les autres autorités compétentes, la Commission et le public.

(97)

Le présent règlement fournit donc un cadre permettant de contraindre à donner aux chercheurs agréés affiliés à un organisme de recherche au sens de l'article 2 de la directive (UE) 2019/790, lesquels organismes peuvent comprendre, aux fins du présent règlement, les organisations de la société civile qui mènent des recherches scientifiques dans le but principal de soutenir leur mission d'intérêt public, l'accès aux données provenant des très grandes plateformes en ligne et des très grands moteurs de recherche en ligne. Il convient que l'ensemble des demandes d'accès aux données en vertu de ce cadre soient proportionnées et protègent de manière appropriée les droits et les intérêts légitimes, y compris les données à caractère personnel, les secrets d'affaires et autres informations confidentielles, de la très grande plateforme en ligne ou du très grand moteur de recherche en ligne et de toute autre partie concernée, y compris les destinataires du service. Toutefois, aux fins de la réalisation de l'objectif du présent règlement, la prise en compte des intérêts commerciaux des fournisseurs ne devrait pas conduire à un refus d'accès aux données nécessaires à l'objectif de recherche spécifique lié à une demande introduite au titre du présent règlement. À cet égard, sans préjudice de la directive (UE) 2016/943 du Parlement européen et du Conseil (32), les fournisseurs devraient garantir un accès approprié aux chercheurs, y compris, si nécessaire, en prenant des mesures de protection technique, par exemple par l'intermédiaire de coffres de données. Les demandes d'accès aux données pourraient, par exemple, porter sur le nombre de vues ou concerner, le cas échéant, d'autres types d'accès aux contenus par les destinataires du service avant leur retrait par les fournisseurs de très grandes plateformes en ligne ou de très grands moteurs de recherche en ligne.

(98)

En outre, lorsque les données sont accessibles au public, ces fournisseurs ne devraient pas empêcher les chercheurs répondant à un sous-ensemble approprié de critères d'utiliser ces données à des fins de recherche qui contribuent à la détection, à la détermination et à la compréhension des risques systémiques. Ils devraient fournir à ces chercheurs l'accès aux données accessibles au public, y compris, lorsque cela est techniquement possible, en temps réel, par exemple les données relatives aux interactions agrégées avec le contenu de pages publiques, de groupes publics ou de personnalités publiques, y compris les données relatives aux impressions et aux échanges, telles que le nombre de réactions, de partages et de commentaires des destinataires du service. Les fournisseurs de très grandes plateformes en ligne ou de très grands moteurs de recherche en ligne devraient être encouragés à coopérer avec les chercheurs et à élargir l'accès aux données pour suivre les préoccupations sociétales grâce à des initiatives volontaires, y compris au moyen d'actions et de procédures convenus dans le cadre de codes de conduite ou de protocoles de crise. Ces fournisseurs et ces chercheurs devraient accorder une attention particulière à la protection des données à caractère personnel et veiller à ce que tout traitement de données à caractère personnel respecte le règlement (UE) 2016/679. Les fournisseurs devraient anonymiser ou pseudonymiser les données à caractère personnel, sauf dans les cas où cela rendrait impossible l'objectif de recherche poursuivi.

(99)

Compte tenu de la complexité du fonctionnement des systèmes déployés et des risques systémiques qu'ils présentent pour la société, il convient que les fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne établissent une fonction de contrôle de la conformité, qui devrait être indépendante des services opérationnels de ces fournisseurs. Le responsable de la fonction de contrôle de la conformité devrait être placé

sous la responsabilité directe de l'organe de direction de ces fournisseurs, y compris en ce qui concerne les préoccupations liées au non-respect du présent règlement. Les responsables de la conformité qui font partie de la fonction de contrôle de la conformité devraient avoir les qualifications, les connaissances, l'expérience et les capacités nécessaires pour mettre en œuvre des mesures et contrôler le respect du présent règlement au sein de l'organisation des fournisseurs de très grandes plateformes en ligne ou de très grands moteurs de recherche en ligne. Les fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne devraient veiller à ce que la fonction de contrôle de la conformité soit associée, d'une manière appropriée et en temps utile, au traitement de toutes les questions relatives au présent règlement, y compris à la stratégie et aux mesures spécifiques d'évaluation et d'atténuation des risques ainsi que, le cas échéant, à l'évaluation du respect des engagements pris par ces fournisseurs en vertu des codes de conduite et des protocoles de crise auxquels ils ont adhéré.

(100)

Compte tenu des risques accrus liés aux activités des fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne ainsi qu'aux obligations supplémentaires qui leur incombent en vertu du présent règlement, d'autres obligations en matière de transparence devraient leur être applicables, notamment l'obligation de faire rapport de manière exhaustive sur les évaluations des risques effectuées et les mesures ultérieures adoptées conformément au présent règlement.

(101)

Il convient que la Commission soit en possession de toutes les ressources, quant au personnel, aux compétences et aux moyens financiers, nécessaires à l'exécution de ses missions au titre du présent règlement. Afin d'assurer la disponibilité des ressources nécessaires à une surveillance adéquate au niveau de l'Union au titre du présent règlement, et étant donné que les États membres devraient être autorisés à imposer une redevance de surveillance aux fournisseurs établis sur leur territoire pour les tâches de surveillance et d'exécution exercées par leurs autorités, la Commission devrait imposer une redevance de surveillance, dont le niveau devrait être établi sur une base annuelle, aux très grandes plateformes en ligne et aux très grands moteurs de recherche en ligne. Le montant global de la redevance de surveillance annuelle imposée devrait être établi sur la base du montant global des coûts supportés par la Commission pour l'exercice de ses missions de surveillance au titre du présent règlement, raisonnablement estimé au préalable. Ce montant devrait englober les coûts liés à l'exercice des compétences et des tâches spécifiques de surveillance, d'enquête, d'exécution et de contrôle à l'égard des fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne, notamment les coûts relatifs à la désignation des très grandes plateformes en ligne et des très grands moteurs de recherche en ligne ou à la création, à la maintenance et à l'exploitation des bases de données envisagées au titre du présent règlement.

Il devrait comprendre également les coûts liés à la mise en place, à la maintenance et à l'exploitation de l'infrastructure institutionnelle et d'information de base aux fins de la coopération entre les coordinateurs pour les services numériques, le comité et la Commission, compte tenu du fait qu'en raison de leur taille et de leur portée, les très grandes plateformes en ligne et les très grands moteurs de recherche en ligne ont une incidence importante sur les ressources nécessaires au fonctionnement de ces infrastructures. L'estimation des coûts globaux devrait tenir compte des coûts de surveillance supportés l'année précédente, y

compris, le cas échéant, des coûts excédant la redevance de surveillance annuelle individuelle imposée l'année précédente. Les recettes affectées externes résultant de la redevance de surveillance annuelle pourraient être utilisées pour financer des ressources humaines supplémentaires, telles que des agents contractuels et des experts nationaux détachés, ainsi que d'autres dépenses liées à l'accomplissement des tâches confiées à la Commission par le présent règlement. La redevance de surveillance annuelle imposée aux fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne devrait être proportionnée à la taille du service, telle qu'elle résulte du nombre de destinataires actifs du service dans l'Union. En outre, la redevance de surveillance annuelle individuelle ne devrait pas dépasser un plafond global pour chaque fournisseur de très grandes plateformes en ligne ou de très grands moteurs de recherche en ligne, compte devant être tenu de la capacité économique du fournisseur du ou des services concernés.

(102)

Pour faciliter l'application efficace et cohérente des obligations prévues par le présent règlement qui peuvent nécessiter une mise en œuvre par des moyens technologiques, il importe de promouvoir des normes volontaires portant sur certaines procédures techniques, lorsque le secteur peut contribuer à la mise au point de moyens normalisés pour aider les fournisseurs de services intermédiaires à se conformer au présent règlement, par exemple en autorisant la soumission de notifications, y compris par des interfaces de programmation d'application, ou des normes relatives aux conditions générales ou des normes en matière d'audit, ou des normes relatives à l'interopérabilité des registres de publicités. En outre, parmi ces normes pourraient figurer des normes relatives à la publicité en ligne, aux systèmes de recommandation, à l'accessibilité et à la protection des mineurs en ligne. Les fournisseurs de services intermédiaires sont libres d'adopter ces normes, mais l'adoption de celles-ci ne présume pas la conformité au présent règlement. Dans le même temps, en fournissant de bonnes pratiques, ces normes pourraient, en particulier, être utiles pour les fournisseurs de services intermédiaires de relativement petite taille. En fonction des cas, ces normes pourraient faire la distinction entre différents types de contenus illicites ou différents types de services intermédiaires.

(103)

Il convient que la Commission et le comité encouragent l'élaboration de codes de conduite volontaires ainsi que la mise en œuvre des dispositions énoncées dans ces codes pour contribuer à l'application du présent règlement. La Commission et le comité devraient se fixer comme objectif que les codes de conduite définissent clairement la nature des objectifs d'intérêt général visés, qu'ils contiennent des mécanismes d'évaluation indépendante de la réalisation de ces objectifs et que le rôle des autorités concernées soit clairement défini. Il convient d'accorder une attention particulière à la prévention des effets négatifs sur la sécurité et à la protection de la vie privée et des données à caractère personnel, ainsi qu'à l'interdiction d'imposer des obligations générales de surveillance. Bien que la mise en œuvre des codes de conduite devrait être mesurable et soumise à un contrôle public, cela ne devrait cependant pas porter atteinte au caractère volontaire de ces codes, ni à la liberté des parties intéressées de décider d'y participer ou non. Dans certaines circonstances, il est important que les très grandes plateformes en ligne coopèrent à l'élaboration de codes de conduite spécifiques et y adhèrent. Aucune disposition du présent règlement n'empêche d'autres fournisseurs de services d'adhérer aux mêmes normes de diligence, d'adopter les bonnes pratiques et de

bénéficier des lignes de conduite fournies par la Commission et le comité, en souscrivant aux mêmes codes de conduite.

(104)

Il convient que le présent règlement détermine certains domaines à prendre en considération pour ces codes de conduite. En particulier, des mesures d'atténuation des risques concernant des types spécifiques de contenu illicite devraient être explorées par le biais d'accords d'autorégulation et de corégulation. Un autre domaine à prendre en considération est celui des éventuelles répercussions négatives des risques systémiques sur la société et la démocratie, tels que la désinformation ou les manipulations et les abus, ou tout effet nocif sur les mineurs. Cela concerne notamment les opérations coordonnées visant à amplifier l'information, y compris la désinformation, comme l'utilisation de robots ou de faux comptes pour la création d'informations intentionnellement inexactes ou trompeuses, parfois dans le but d'obtenir un gain économique, opérations qui sont particulièrement préjudiciables aux destinataires vulnérables du service, tels que les mineurs. Dans ces domaines, l'adhésion à un code de conduite donné et son respect par une très grande plateforme en ligne ou un très grand moteur de recherche en ligne peuvent être considérés comme constituant une mesure appropriée d'atténuation des risques. Le refus, sans explications valables, par le fournisseur d'une plateforme en ligne ou d'un moteur de recherche en ligne de l'invitation de la Commission à participer à l'application d'un tel code de conduite pourrait être pris en compte, le cas échéant, pour déterminer si la plateforme en ligne ou le moteur de recherche en ligne a enfreint les obligations prévues dans le présent règlement. Le simple fait d'adhérer à un code de conduite donné et de le mettre en œuvre ne devrait pas en lui-même faire présumer que le présent règlement est respecté.

(105)

Les codes de conduite devraient accroître l'accessibilité des très grandes plateformes en ligne et des très grands moteurs de recherche en ligne, dans le respect du droit de l'Union et du droit national, afin de faciliter leur utilisation prévisible par les personnes handicapées. Les codes de conduite pourraient notamment faire en sorte que les informations soient présentées d'une manière perceptible, utilisable, compréhensible et claire et que les formulaires et mesures prévus dans le présent règlement soient faciles à trouver et accessibles aux personnes handicapées.

(106)

Les règles relatives aux codes de conduite prévues par le présent règlement pourraient servir de base aux efforts d'autorégulation déjà déployés au niveau de l'Union, notamment l'engagement en matière de sécurité des produits, le protocole d'accord sur la vente de contrefaçons sur l'internet, le code de conduite pour la lutte contre les discours haineux illégaux en ligne ainsi que le code de bonnes pratiques en matière de désinformation. En ce qui concerne ce dernier en particulier, conformément aux orientations de la Commission le code de bonnes pratiques en matière de désinformation a été renforcé, comme annoncé dans le plan d'action pour la démocratie européenne.

(107)

La fourniture de publicité en ligne implique généralement plusieurs acteurs, notamment des services intermédiaires qui mettent en relation les éditeurs de publicité et les annonceurs. Les codes de conduite devraient soutenir et compléter les obligations en matière de transparence relatives à la publicité pesant sur les fournisseurs de plateformes en ligne, de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne énoncées dans le présent règlement afin de prévoir des mécanismes souples et efficaces visant à faciliter et à renforcer le respect de ces obligations, notamment en ce qui concerne les modalités de transmission des informations pertinentes. Il devrait notamment s'agir de faciliter la transmission des informations sur l'annonceur qui paie la publicité lorsqu'il diffère de la personne physique ou morale pour le compte de laquelle la publicité est présentée sur l'interface en ligne d'une plateforme en ligne. Les codes de conduite devraient également comprendre des mesures visant à garantir que des informations utiles sur la monétisation des données sont correctement partagées tout au long de la chaîne de valeur. La participation d'un large éventail de parties prenantes devrait garantir que ces codes de conduite bénéficient d'un large soutien, sont techniquement solides, efficaces et offrent le plus haut niveau de facilité d'utilisation afin que les obligations en matière de transparence atteignent leurs objectifs. Afin de garantir l'efficacité des codes de conduite, la Commission devrait prévoir des mécanismes d'évaluation lors de l'élaboration des codes de conduite. Le cas échéant, la Commission peut inviter l'Agence des droits fondamentaux ou le Contrôleur européen de la protection des données à donner son avis sur le code de conduite qui le concerne.

(108)

Outre le mécanisme de réaction aux crises pour les très grandes plateformes en ligne et les très grands moteurs de recherche en ligne, la Commission peut entreprendre l'élaboration de protocoles de crise volontaires pour coordonner une réponse rapide, collective et transfrontière dans l'environnement en ligne. Cela peut ainsi être le cas lorsque les plateformes en ligne sont utilisées de manière abusive, par exemple, pour la diffusion rapide de contenus illicites ou de désinformation ou lorsqu'il est nécessaire de diffuser rapidement des informations fiables. Compte tenu du rôle important des très grandes plateformes en ligne dans la diffusion de l'information dans nos sociétés et au-delà des frontières, il convient d'encourager les fournisseurs de ces plateformes à élaborer et à appliquer des protocoles de crise spécifiques. Ces protocoles de crise ne devraient être activés que pour une période limitée et les mesures adoptées devraient également être limitées à ce qui est strictement nécessaire pour faire face à la circonstance extraordinaire considérée. Ces mesures devraient être cohérentes avec le présent règlement et ne devraient pas constituer, pour les fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne participants, une obligation générale de surveiller les informations qu'ils transmettent ou stockent, ni de rechercher activement des faits ou des circonstances indiquant un contenu illicite.

(109)

Afin de contrôler et de faire respecter de manière adéquate les obligations prévues par le présent règlement, les États membres devraient désigner au moins une autorité qui serait chargée de surveiller l'application du présent règlement et de le faire respecter, sans préjudice de la possibilité de désigner une autorité existante ni de la forme juridique de celle-ci conformément au droit national. En fonction de leur structure constitutionnelle, organisationnelle et administrative nationale, les États membres devraient toutefois pouvoir confier des missions et des pouvoirs spécifiques de surveillance ou d'exécution en ce qui

concerne l’application du présent règlement à plusieurs autorités compétentes, par exemple dans des secteurs spécifiques où des autorités existantes peuvent également être chargées de ces tâches, telles que les régulateurs des communications électroniques, les régulateurs des médias ou les autorités chargées de la protection des consommateurs. Dans l’exécution de leurs missions, toutes les autorités compétentes devraient contribuer à la réalisation des objectifs du présent règlement, à savoir le bon fonctionnement du marché intérieur des services intermédiaires, au sein duquel des règles harmonisées pour un environnement en ligne sûr, prévisible et fiable, propice à l’innovation, et en particulier les obligations de diligence applicables aux différentes catégories de fournisseurs de services intermédiaires, font l’objet d’une surveillance et d’une mise en application effectives, aux fins d’une protection efficace des droits fondamentaux consacrés dans la Charte, dont notamment le principe de protection des consommateurs. Le présent règlement n’impose pas aux États membres de confier aux autorités compétentes la mission de se prononcer sur la licéité d’éléments de contenus spécifiques.

(110)

Compte tenu de la nature transfrontière des services en cause et de la portée horizontale des obligations introduites par le présent règlement, une autorité désignée pour surveiller l’application du présent règlement et, si nécessaire, le faire respecter devrait être désignée en tant que coordinateur pour les services numériques dans chaque État membre. Lorsque plusieurs autorités compétentes sont désignées pour surveiller l’application du présent règlement et le faire respecter, une seule autorité dans cet État membre devrait être désignée en tant que coordinateur pour les services numériques. Il convient que le coordinateur pour les services numériques fasse office de point de contact unique concernant toutes les questions liées à l’application du présent règlement pour la Commission, le comité, les coordinateurs pour les services numériques des autres États membres, ainsi que pour les autres autorités compétentes de l’État membre en question. En particulier, lorsque, dans un État membre donné, plusieurs autorités compétentes sont chargées de missions au titre du présent règlement, le coordinateur pour les services numériques devrait assurer la coordination et la coopération avec ces autorités conformément aux dispositions du droit national fixant leurs missions respectives et sans préjudice de l’évaluation indépendante des autres autorités compétentes. Sans que cela ne suppose une supériorité hiérarchique sur d’autres autorités compétentes dans l’exercice de leurs missions, le coordinateur pour les services numériques devrait veiller à une participation effective de toutes les autorités compétentes concernées et faire rapport en temps utile sur leur évaluation dans le cadre de la coopération en matière de surveillance et d’exécution au niveau de l’Union. De plus, en complément des mécanismes spécifiques prévus dans le présent règlement en ce qui concerne la coopération au niveau de l’Union, l’État membre devrait également veiller à la coopération entre le coordinateur pour les services numériques et les autres autorités compétentes désignées au niveau national, le cas échéant, au moyen d’instruments appropriés, tels que la mise en commun des ressources, des groupes de travail communs, des enquêtes communes et des mécanismes d’assistance mutuelle.

(111)

Le coordinateur pour les services numériques, de même que les autorités compétentes désignées en vertu du présent règlement, jouent un rôle crucial pour assurer l’effectivité des droits et obligations prévus par le présent règlement et la réalisation de ses objectifs. En conséquence, il est nécessaire de veiller à ce que ces autorités disposent des moyens

nécessaires, y compris des ressources financières et humaines, pour surveiller tous les fournisseurs de services intermédiaires relevant de leur compétence, dans l'intérêt de tous les citoyens de l'Union. Compte tenu de la diversité des fournisseurs de services intermédiaires et du fait qu'ils utilisent des technologies avancées pour fournir leurs services, il est également essentiel que le coordinateur pour les services numériques et les autorités compétentes concernées soient dotés du nombre nécessaire d'agents et d'experts possédant des compétences spécialisées et des moyens techniques avancés, et qu'ils gèrent de manière autonome les ressources financières requises pour s'acquitter de leurs missions. En outre, le niveau des ressources devrait être adapté à la taille, à la complexité et à l'impact potentiel sur la société des fournisseurs de services intermédiaires relevant de leur compétence, ainsi qu'à la portée de leurs services dans l'Union. Le présent règlement est sans préjudice de la possibilité pour les États membres d'établir des mécanismes de financement fondés sur une redevance de surveillance imposée aux fournisseurs de services intermédiaires en vertu du droit national en conformité avec le droit de l'Union, pour autant qu'elle soit perçue auprès de fournisseurs de services intermédiaires ayant leur établissement principal dans l'État membre en question, qu'elle soit strictement limitée à ce qui est nécessaire et proportionné pour couvrir les coûts liés à l'accomplissement des tâches confiées aux autorités compétentes en vertu du présent règlement, à l'exclusion des tâches confiées à la Commission, et qu'une transparence suffisante soit assurée quant à la perception et à l'utilisation d'une telle redevance de surveillance.

(112)

Les autorités compétentes désignées au titre du présent règlement devraient également agir en toute indépendance par rapport aux organismes privés et publics, sans obligation ni possibilité de solliciter ou de recevoir des instructions, y compris du gouvernement, et sans préjudice des obligations spécifiques de coopérer avec d'autres autorités compétentes, les coordinateurs pour les services numériques, le comité et la Commission. Toutefois, l'indépendance desdites autorités ne devrait pas signifier qu'elles ne peuvent pas être soumises, dans le respect des constitutions nationales et sans que cela mette en péril la réalisation des objectifs du présent règlement, à des mécanismes de responsabilisation proportionnés portant sur les activités générales des coordinateurs pour les services numériques, telles que leurs dépenses financières ou la présentation de rapports aux parlements nationaux. L'exigence d'indépendance ne devrait pas non plus faire obstacle à l'exercice d'un contrôle juridictionnel ni à la possibilité de consulter d'autres autorités nationales, y compris, le cas échéant, les autorités répressives, les autorités de gestion des crises ou les autorités chargées de la protection des consommateurs, ou de procéder à des échanges de vues réguliers avec ces autorités pour se tenir mutuellement informées des enquêtes en cours, sans porter atteinte à l'exercice de leurs pouvoirs respectifs.

(113)

Les États membres peuvent désigner une autorité nationale existante pour assumer la fonction de coordinateur pour les services numériques ou lui confier les missions spécifiques de surveiller l'application du présent règlement et de le faire respecter, à condition que cette autorité désignée respecte les exigences fixées dans le présent règlement, notamment en ce qui concerne son indépendance. En outre, il n'est en principe pas exclu que les États membres puissent procéder à un regroupement de fonctions au sein d'une autorité existante, dans le respect du droit de l'Union. Les mesures à cet effet peuvent comprendre, entre autres, l'interdiction de révoquer le président ou un membre du conseil d'administration d'un organe

collégial d'une autorité existante avant l'expiration de leur mandat, au seul motif qu'une réforme institutionnelle a eu lieu impliquant le regroupement de différentes fonctions au sein d'une autorité, en l'absence de règles garantissant que ces révocations ne compromettent pas l'indépendance et l'impartialité de ces membres.

(114)

Les États membres devraient doter le coordinateur pour les services numériques, et toute autre autorité compétente désignée en vertu du présent règlement, de pouvoirs et de moyens suffisants pour rendre effectives leurs activités en matière d'enquête et de d'exécution, conformément aux missions qui leur sont confiées. Cela comprend le pouvoir des autorités compétentes d'adopter des mesures provisoires conformément au droit national en cas de risque de préjudice grave. Ces mesures provisoires, qui peuvent inclure des injonctions de mettre fin ou de remédier à une infraction alléguée donnée, ne devraient pas aller au-delà de ce qui est nécessaire pour veiller à ce qu'un préjudice grave soit évité dans l'attente de la décision définitive. Il convient notamment que le coordinateur pour les services numériques puisse rechercher et obtenir des informations qui se trouvent sur le territoire de son État membre, y compris dans le cadre d'enquêtes conjointes, en tenant dûment compte du fait que les mesures de surveillance et d'exécution concernant un fournisseur relevant de la compétence d'un autre État membre ou de la Commission devraient être adoptées par le coordinateur pour les services numériques de cet autre État membre, le cas échéant conformément aux procédures relatives à la coopération transfrontière, ou, selon le cas, par la Commission.

(115)

Conformément au droit de l'Union et en particulier au présent règlement et à la Charte, les États membres devraient définir en détail dans leur droit national les conditions et limites de l'exercice des pouvoirs d'enquête et d'exécution de leurs coordinateurs pour les services numériques, et, le cas échéant, d'autres autorités compétentes au titre du présent règlement.

(116)

Dans l'exercice de ces pouvoirs, les autorités compétentes devraient respecter les règles nationales applicables concernant les procédures et les aspects tels que la nécessité de disposer d'une autorisation judiciaire préalable pour pénétrer dans certains locaux ainsi que le secret professionnel. Ces dispositions devraient en particulier garantir le respect des droits fondamentaux à un recours effectif et à un procès équitable, y compris les droits de la défense, ainsi que du droit au respect de la vie privée. À cet égard, les garanties prévues en ce qui concerne les procédures de la Commission en vertu du présent règlement pourraient constituer une référence appropriée. Avant qu'une décision définitive soit prise, il convient de garantir une procédure préalable, équitable et impartiale, y compris le droit des personnes concernées d'être entendues et d'avoir accès au dossier, dans le respect de la confidentialité et du secret professionnel et d'affaires, ainsi que de l'obligation de dûment motiver les décisions. Toutefois, cela ne devrait pas empêcher que des mesures soient prises, dans des cas d'urgence dûment justifiés et sous réserve de conditions et de modalités procédurales appropriées. Il convient que l'exercice de ces pouvoirs soit également proportionné, entre autres, à la nature de l'infraction ou de l'infraction présumée et au préjudice global, réel ou potentiel, qui en découle. Les autorités compétentes devraient tenir compte de tous les faits et circonstances

pertinents de l’affaire, y compris des informations recueillies par les autorités compétentes d’autres États membres.

(117)

Les États membres devraient veiller à ce que les infractions aux obligations prévues par le présent règlement puissent être sanctionnés d’une manière efficace, proportionnée et dissuasive, en fonction de la nature, de la gravité, de la récurrence et de la durée de l’infraction, compte tenu de l’objectif d’intérêt général poursuivi, de l’ampleur et de la nature des activités menées, ainsi que de la capacité économique de l’auteur de l’infraction. En particulier, les sanctions devraient tenir compte du fait que le fournisseur de services intermédiaires concerné manque systématiquement ou de manière récurrente aux obligations qui lui incombent en vertu du présent règlement, ainsi que, le cas échéant, du nombre de destinataires du service affectés, du caractère intentionnel ou négligent de l’infraction et du fait que le fournisseur exerce ses activités dans plusieurs États membres. Lorsque le présent règlement prévoit un montant maximal pour les amendes ou les astreintes, ce montant maximal devrait s’appliquer pour chaque infraction au présent règlement et sans préjudice de la modulation des amendes ou des astreintes en ce qui concerne des infractions spécifiques. Les États membres devraient veiller à ce que l’imposition d’amendes ou d’astreintes en cas d’infraction soit effective, proportionnée et dissuasive dans chaque cas particulier en établissant des règles et procédures nationales conformément au présent règlement, en tenant compte de tous les critères concernant les conditions générales d’imposition des amendes ou des astreintes.

(118)

Afin de garantir l’exécution effective des obligations fixées dans le présent règlement, il convient que les particuliers ou les organisations représentatives puissent introduire toute plainte relative au respect de ces obligations auprès du coordinateur pour les services numériques du territoire où ils ont été destinataires du service, sans préjudice des règles du présent règlement en matière de répartition des compétences et des règles applicables en matière de traitement des plaintes conformément aux principes nationaux de bonne administration. Les plaintes pourraient donner un aperçu fidèle des préoccupations suscitées par un fournisseur de services intermédiaire déterminé quant au respect du présent règlement et pourraient également informer le coordinateur pour les services numériques de toute autre question de nature transversale. Le coordinateur pour les services numériques devrait impliquer d’autres autorités nationales compétentes ainsi que le coordinateur pour les services numériques d’un autre État membre, et en particulier celui de l’État membre où le fournisseur de services intermédiaires concerné est établi, si la question nécessite une coopération transfrontière.

(119)

Les États membres devraient veiller à ce que les coordinateurs pour les services numériques puissent prendre des mesures qui permettent de lutter effectivement contre certaines infractions particulièrement graves et persistantes au présent règlement et qui soient proportionnées auxdites infractions. Il convient d’exiger, en particulier lorsque ces mesures sont susceptibles de porter atteinte aux droits et intérêts de tiers, comme cela peut être le cas notamment lorsque l’accès à des interfaces en ligne est restreint, que lesdites mesures soient assorties de garanties supplémentaires En particulier, les tiers potentiellement affectés

devraient avoir la possibilité d'être entendus et ces injonctions ne devraient être émises que lorsqu'il n'est pas raisonnablement possible de recourir aux pouvoirs conférés par d'autres actes du droit de l'Union ou du droit national pour adopter de telles mesures, par exemple pour protéger les intérêts collectifs des consommateurs, pour assurer le retrait rapide des pages internet contenant ou diffusant de la pédopornographie ou pour rendre impossible l'accès à des services qui sont utilisés par un tiers pour porter atteinte à un droit de propriété intellectuelle.

(120)

Une telle injonction visant à restreindre l'accès ne devrait pas excéder ce qui est nécessaire pour atteindre l'objectif poursuivi. À cette fin, elle devrait être temporaire et être destinée, en principe à un fournisseur de services intermédiaires, tel que le fournisseur de services d'hébergement concerné, le fournisseur de services internet, le registre du domaine ou le bureau d'enregistrement concerné, qui est raisonnablement en mesure d'atteindre cet objectif sans restreindre indûment l'accès aux informations licites.

(121)

Sans préjudice des dispositions relatives à l'exemption de responsabilité prévues dans le présent règlement en ce qui concerne les informations transmises ou stockées à la demande d'un destinataire du service, un fournisseur de services intermédiaires devrait être tenu responsable des préjudices subis par les destinataires du service causés par une violation par ledit fournisseur des obligations énoncées dans le présent règlement. L'indemnisation devrait se faire conformément aux règles et procédures définies dans le droit national applicable et sans préjudice d'autres possibilités de recours prévues par les règles relatives à la protection des consommateurs.

(122)

Il convient que le coordinateur pour les services numériques publie régulièrement, par exemple sur son site internet, un rapport sur les activités menées au titre du présent règlement. En particulier, le rapport devrait être publié dans un format lisible par une machine et comporter un aperçu des plaintes reçues et de leur suivi, notamment le nombre global de plaintes reçues et le nombre de plaintes ayant conduit à l'ouverture d'une enquête formelle ou à une transmission à d'autres coordinateurs pour les services numériques, sans faire référence à des données à caractère personnel. Dans la mesure où le coordinateur pour les services numériques est également informé des injonctions d'agir contre des contenus illicites ou de fournir, par l'intermédiaire du système de partage d'informations, des informations régies par le présent règlement, il devrait inclure dans son rapport annuel le nombre et les catégories d'injonctions de ce type émises à l'encontre des fournisseurs de services intermédiaires par les autorités judiciaires et administratives de son État membre.

(123)

Par souci de clarté, de simplicité et d'efficacité, les pouvoirs de surveillance et d'exécution des obligations prévues au présent règlement devraient être conférés aux autorités compétentes de l'État membre dans lequel se trouve l'établissement principal du fournisseur de services intermédiaires, c'est-à-dire dans lequel le fournisseur a son administration centrale ou son siège statutaire au sein duquel sont exercés les principales fonctions financières ainsi

que le contrôle opérationnel. En ce qui concerne les fournisseurs qui ne sont pas établis dans l'Union, mais qui proposent des services dans l'Union et relèvent donc du champ d'application du présent règlement, l'État membre dans lequel ces fournisseurs ont désigné leur représentant légal devrait être compétent, compte tenu de la fonction de représentant légal prévue par le présent règlement. Toutefois, dans l'intérêt d'une application effective du présent règlement, lorsqu'un fournisseur n'a pas désigné de représentant légal, tous les États membres ou la Commission, selon le cas, devraient être compétents. Cette compétence peut être exercée par toute autorité compétente ou la Commission, pour autant que le fournisseur ne fasse pas l'objet d'une procédure d'exécution portant sur les mêmes faits par une autre autorité compétente ou la Commission. Afin que le principe non bis in idem soit respecté, et notamment afin d'éviter que la même infraction aux obligations définies dans le présent règlement ne soit sanctionnée plus d'une fois, chaque État membre qui entend exercer sa compétence à l'égard de tels fournisseurs devrait, sans retard injustifié, en informer toutes les autres autorités, y compris la Commission, au moyen du système de partage d'informations mis en place aux fins du présent règlement.

(124)

Compte tenu de leur effet potentiel et des difficultés que comporte leur surveillance effective, des règles spéciales de surveillance et d'exécution sont nécessaires à l'égard des fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne. La Commission devrait être chargée, le cas échéant avec le concours des autorités nationales compétentes, de surveiller et de faire respecter par les autorités publiques l'obligation de gérer les questions systémiques, notamment les questions ayant un impact important sur les intérêts collectifs des destinataires du service. Par conséquent, la Commission devrait disposer de pouvoirs exclusifs de surveillance et d'exécution des obligations supplémentaires de gestion des risques systémiques imposées aux fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne par le présent règlement. Les pouvoirs exclusifs de la Commission devraient s'entendre sans préjudice de certaines tâches administratives confiées par le présent règlement aux autorités compétentes des États membres d'établissement, telles que l'agrément des chercheurs.

(125)

Les pouvoirs de surveillance et d'exécution des obligations de diligence, autres que les obligations supplémentaires de gestion des risques systémiques imposées par le présent règlement aux fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne, devraient être partagés par la Commission et les autorités nationales compétentes. D'une part, la Commission pourrait très souvent être mieux placée pour remédier aux infractions systémiques commises par ces fournisseurs, comme les infractions qui touchent plusieurs États membres, les infractions graves répétées ou l'absence de mise en place des mécanismes efficaces requis par le présent règlement. D'autre part, les autorités compétentes de l'État membre dans lequel se trouve l'établissement principal d'un fournisseur d'une très grande plateforme en ligne ou d'un très grand moteur de recherche en ligne pourraient être mieux placées pour remédier aux infractions particulières commises par ces fournisseurs lorsqu'elles ne soulèvent pas de questions systémiques ou transfrontières. Dans un souci d'efficience, afin d'éviter les doubles emplois et de veiller au respect du principe non bis in idem, c'est à la Commission qu'il devrait appartenir d'évaluer si elle juge approprié d'exercer ces compétences partagées dans un cas donné et, lorsqu'elle a engagé la procédure, les États membres ne devraient plus avoir la faculté de le faire. Les États membres devraient

coopérer étroitement à la fois entre eux et avec la Commission et la Commission devrait coopérer étroitement avec les États membres afin d'assurer le bon fonctionnement et l'efficacité du système de surveillance et d'exécution mis en place par le présent règlement.

(126)

Les règles de répartition des compétences prévues par le présent règlement devraient s'appliquer sans préjudice des dispositions du droit de l'Union et des règles nationales de droit international privé relatives à la juridiction et à la loi applicable en matière civile et commerciale, telles que les procédures engagées par des consommateurs devant les juridictions de l'État membre où ils sont domiciliés conformément aux dispositions pertinentes du droit de l'Union. En ce qui concerne les obligations, imposées aux fournisseurs de services intermédiaires par le présent règlement, d'informer l'autorité d'émission de la suite donnée aux injonctions d'agir contre des contenus illicites et aux injonctions de fournir des informations, les règles de répartition des compétences ne devraient s'appliquer qu'à la surveillance du respect de ces obligations, mais pas aux autres aspects de l'injonction, telle que la compétence d'émettre l'injonction.

(127)

Compte tenu de l'aspect transfrontière et transsectoriel des services intermédiaires, une coopération à haut niveau est nécessaire pour veiller à l'application cohérente du présent règlement et à la disponibilité des informations pertinentes pour l'exercice des tâches d'exécution par l'intermédiaire du système de partage d'informations. La coopération peut prendre différentes formes en fonction des questions en jeu, sans préjudice des exercices d'enquêtes communes. Il est en tout état de cause nécessaire que le coordinateur pour les services numériques de l'État membre d'établissement d'un fournisseur de services intermédiaires informe les autres coordinateurs pour les services numériques des questions et des enquêtes concernant un fournisseur et des mesures qui vont être prises à l'égard de ce fournisseur. En outre, lorsqu'une autorité compétente d'un État membre détient des informations pertinentes pour une enquête menée par les autorités compétentes de l'État membre d'établissement, ou est en mesure de recueillir sur son territoire de telles informations auxquelles les autorités compétentes de l'État membre d'établissement n'ont pas accès, le coordinateur pour les services numériques de l'État membre de destination devrait prêter son concours en temps utile au coordinateur pour les services numériques de l'État membre d'établissement, y compris dans le cadre de l'exercice de ses pouvoirs d'enquête conformément aux procédures nationales applicables et à la Charte. Le destinataire de ces mesures d'enquête devrait s'y conformer et être tenu responsable en cas de manquement, et les autorités compétentes de l'État membre d'établissement devraient pouvoir se fier aux informations recueillies dans le cadre de l'assistance mutuelle, afin de garantir le respect du présent règlement.

(128)

Le coordinateur pour les services numériques de l'État membre de destination, en particulier sur la base de plaintes reçues ou, le cas échéant, de la contribution d'autres autorités nationales compétentes ou du comité, dans le cas de questions concernant plus de trois États membres, devrait pouvoir demander au coordinateur pour les services numériques de l'État membre d'établissement de prendre des mesures d'enquête ou d'exécution à l'égard d'un fournisseur relevant de sa compétence. Ces demandes de mesures devraient reposer sur des

éléments de preuve bien étayés démontrant l'existence d'une infraction alléguée ayant une incidence négative sur les intérêts collectifs des destinataires du service dans son État membre ou ayant une incidence négative pour la société. Le coordinateur pour les services numériques de l'État membre d'établissement devrait pouvoir recourir à l'assistance mutuelle ou inviter le coordinateur pour les services numériques demandeur à participer à une enquête commune si des informations supplémentaires sont nécessaires pour prendre une décision, sans qu'il soit fait obstacle à la possibilité d'inviter la Commission à évaluer le cas s'il a des raisons de soupçonner qu'une infraction systémique commise par une très grande plateforme en ligne ou un très grand moteur de recherche en ligne puisse être en cause.

(129)

Il convient que le comité puisse saisir la Commission s'il n'est pas d'accord avec les évaluations ou les mesures prises ou proposées ou si aucune mesure n'a été prise conformément au présent règlement à la suite d'une demande de coopération transfrontière ou d'enquête commune. Lorsque la Commission, sur la base des informations mises à disposition par les autorités concernées, considère que les mesures proposées, y compris le niveau des amendes proposé, ne permettent pas de garantir l'exécution effective des obligations prévues dans le présent règlement, elle devrait par conséquent pouvoir exprimer ses sérieux doutes et demander au coordinateur pour les services numériques compétent de réévaluer la question et de prendre, dans un délai déterminé, les mesures nécessaires pour assurer le respect du présent règlement. Cette possibilité est sans préjudice de l'obligation générale faite à la Commission de surveiller l'application du droit de l'Union et, si nécessaire, de le faire respecter, sous le contrôle de la Cour de justice de l'Union européenne, conformément aux traités.

(130)

Afin de faciliter la surveillance et les enquêtes transfrontières portant sur les obligations fixées dans le présent règlement impliquant plusieurs États membres, les coordinateurs pour les services numériques de l'État membre d'établissement devraient pouvoir, par l'intermédiaire du système de partage d'informations, inviter d'autres coordinateurs pour les services numériques à participer à une enquête commune concernant une infraction alléguée au présent règlement. D'autres coordinateurs pour les services numériques et, le cas échéant, d'autres autorités compétentes devraient pouvoir prendre part à l'enquête proposée par le coordinateur pour les services numériques de l'État membre d'établissement, à moins que ce dernier ne considère qu'un nombre excessif d'autorités participantes risque de nuire à l'efficacité de l'enquête compte tenu des caractéristiques de l'infraction alléguée et de l'absence d'effets directs sur les destinataires du service dans ces États membres. Les activités menées dans le cadre des enquêtes communes peuvent comprendre des mesures très diverses qui doivent être coordonnées par le coordinateur pour les services numériques de l'État membre d'établissement conformément aux disponibilités des autorités participantes, telles que des exercices de collecte coordonnée de données, la mise en commun des ressources, des groupes de travail, des demandes coordonnées d'informations ou des inspections communes de locaux. Toutes les autorités compétentes participant à une enquête commune devraient coopérer avec le coordinateur pour les services numériques de l'État membre d'établissement, notamment en exerçant leurs pouvoirs d'enquête sur leur territoire, conformément aux procédures nationales applicables. L'enquête commune devrait se conclure dans un délai déterminé par un rapport final tenant compte de la contribution de toutes les autorités compétentes participantes. Le comité peut également, à la demande d'au moins trois coordinateurs pour les services numériques d'États membres de destination, recommander à

un coordinateur pour les services numériques d'un État membre d'établissement de lancer une telle enquête commune et donner des indications sur son organisation. Afin d'éviter les blocages, le comité devrait pouvoir saisir la Commission dans des cas précis, notamment lorsque le coordinateur pour les services numériques de l'État membre d'établissement refuse de lancer l'enquête et que le comité n'est pas d'accord avec la justification donnée.

(131)

Afin d'assurer une application cohérente du présent règlement, il est nécessaire de créer un groupe consultatif indépendant au niveau de l'Union, un comité européen pour les services numériques, qui devrait soutenir la Commission et aider à coordonner les actions des coordinateurs pour les services numériques. Le comité devrait être composé des coordinateurs pour les services numériques, lorsque ceux-ci ont été désignés, sans préjudice de la possibilité pour ces derniers d'inviter à ses réunions ou de nommer des délégués ad hoc d'autres autorités compétentes chargées de tâches spécifiques au titre du présent règlement, lorsque cela est nécessaire en vertu de la répartition nationale des tâches et des compétences. Si plusieurs participants d'un État membre sont présents, le droit de vote devrait rester limité à une voix par État membre.

(132)

Le comité devrait contribuer à définir une vision commune de l'Union concernant l'application cohérente du présent règlement et à la coopération entre les autorités compétentes, notamment en conseillant la Commission et les coordinateurs pour les services numériques sur les mesures d'enquête et d'exécution appropriées, en particulier à l'égard des fournisseurs de très grandes plateformes en ligne ou de très grands moteurs de recherche en ligne et compte tenu, notamment, de la liberté des fournisseurs de services intermédiaire de fournir des services dans toute l'Union. Le comité devrait également contribuer à l'élaboration de modèles et de codes de conduite pertinents et à l'analyse des nouvelles tendances générales qui se dessinent dans le développement des services numériques dans l'Union, notamment en émettant des avis ou des recommandations sur les questions ayant trait aux normes.

(133)

À cette fin, le comité devrait pouvoir adopter des avis, des demandes et des recommandations adressés aux coordinateurs pour les services numériques ou à d'autres autorités nationales compétentes. Bien que ces actes ne soient pas juridiquement contraignants, toute décision de s'en écarter devrait être assortie d'une explication adéquate et pourrait être prise en compte par la Commission lors de l'évaluation du respect du présent règlement par l'État membre concerné.

(134)

Le comité devrait réunir les représentants des coordinateurs pour les services numériques et éventuellement d'autres autorités compétentes sous la présidence de la Commission, en vue de garantir, pour l'évaluation des questions qui lui sont soumises, une dimension pleinement européenne. Eu égard à d'éventuels éléments de nature transversale susceptibles de présenter un intérêt pour d'autres cadres réglementaires au niveau de l'Union, le comité devrait être autorisé à coopérer avec d'autres organes, organismes, agences et groupes consultatifs de

l’Union ayant des responsabilités dans des domaines tels que l’égalité, y compris l’égalité des genres, la non-discrimination, la protection des données, les communications électroniques, les services audiovisuels, la détection des fraudes au détriment du budget de l’Union en matière de droits de douane et les enquêtes en la matière, la protection des consommateurs ou le droit de la concurrence, dans la mesure où cela est nécessaire à l’accomplissement de ses tâches.

(135)

La Commission, par l’intermédiaire du président, devrait participer au comité sans droit de vote. Par l’intermédiaire du président, la Commission devrait veiller à ce que l’ordre du jour des réunions soit établi conformément aux demandes des membres du comité, comme le prévoit le règlement intérieur, et conformément aux tâches du comité telles qu’elles sont définies dans le présent règlement.

(136)

Ses activités devant bénéficier d’un soutien, il convient que le comité puisse s’appuyer sur les compétences et les ressources humaines de la Commission et des autorités nationales compétentes. Il y a lieu de préciser les modalités opérationnelles spécifiques du fonctionnement interne du comité dans le règlement intérieur de celui-ci.

(137)

Compte tenu de l’importance des très grandes plateformes en ligne ou des très grands moteurs de recherche en ligne, eu égard à leur portée et à leur poids, leur manquement aux obligations spécifiques qui leur sont applicables est susceptible d’affecter un nombre substantiel de destinataires des services dans différents États membres et peut causer des préjudices importants à la société, alors même qu’il peut aussi être particulièrement complexe de détecter ces manquements et d’y remédier. Pour ce motif, la Commission devrait, en coopération avec les coordinateurs pour les services numériques et le comité, développer l’expertise et les capacités de l’Union en ce qui concerne la surveillance des très grandes plateformes en ligne et des très grands moteurs de recherche en ligne. Le Commission devrait donc être en mesure de coordonner et d’utiliser l’expertise et les ressources de ces autorités, par exemple en analysant, à titre permanent ou temporaire, les tendances spécifiques ou les questions qui émergent en ce qui concerne une ou plusieurs très grandes plateformes en ligne ou un ou plusieurs très grands moteurs de recherche en ligne. Les États membres devraient coopérer avec la Commission au développement de ces capacités, notamment par le détachement de personnel, le cas échéant, et la contribution à la mise en place d’une capacité commune de surveillance propre à l’Union. Afin de développer l’expertise et les capacités de l’Union, la Commission peut également recourir à l’expertise et aux capacités de l’Observatoire de l’économie des plateformes en ligne, institué par la décision de la Commission du 26 avril 2018 relative à la création du groupe d’experts de l’Observatoire de l’économie des plateformes en ligne, d’organismes spécialisés pertinents et de centres d’excellence. La Commission peut inviter des experts possédant une expertise spécifique, y compris des chercheurs agréés, des représentants d’agences et d’organismes de l’Union, des représentants du secteur, des associations représentant les utilisateurs ou la société civile, des organisations internationales, des experts du secteur privé ainsi que d’autres parties prenantes.

(138)

La Commission devrait pouvoir enquêter de sa propre initiative sur les infractions conformément aux pouvoirs prévus dans le présent règlement, y compris en demandant à avoir accès à des données, en exigeant des informations ou en menant des inspections, ainsi qu'en faisant appel au soutien des coordinateurs pour les services numériques. Lorsque la surveillance exercée par les autorités nationales compétentes à l'égard de certaines infractions particulières alléguées, commises par des fournisseurs de très grandes plateformes en ligne ou de très grands moteurs de recherche en ligne révèle des questions systémiques, telles que des questions ayant un impact important sur les intérêts collectifs des destinataires du service, les coordinateurs pour les services numériques devraient pouvoir, sur la base d'une demande dûment motivée, saisir la Commission de ces questions. Cette demande devrait comprendre, au minimum, tous les faits et circonstances nécessaires à l'appui de l'infraction alléguée et de son caractère systémique. En fonction du résultat de sa propre évaluation, la Commission devrait pouvoir également prendre les mesures d'enquête et d'exécution nécessaires au titre du présent règlement, y compris, s'il y a lieu, lancer une enquête ou prendre des mesures provisoires.

(139)

Pour pouvoir s'acquitter efficacement de ses tâches, la Commission devrait conserver une marge d'appréciation en ce qui concerne la décision d'engager une procédure à l'encontre de fournisseurs de très grandes plateformes en ligne ou de très grands moteurs de recherche en ligne. Dès lors que la Commission a engagé la procédure, les coordinateurs pour les services numériques des États membres d'établissement concernés devraient être mis dans l'impossibilité d'exercer leurs pouvoirs d'enquête et d'exécution en ce qui concerne le comportement en cause du fournisseur de la très grande plateforme en ligne ou du très grand moteur de recherche en ligne, afin d'éviter les doubles emplois, les incohérences et les risques du point de vue du principe non bis in idem. La Commission devrait toutefois pouvoir demander aux coordinateurs pour les services numériques une contribution individuelle ou commune à l'enquête. Conformément au principe de coopération loyale, il convient que le coordinateur pour les services numériques mette tout en œuvre pour satisfaire les demandes justifiées et proportionnées adressées par la Commission dans le cadre d'une enquête. En outre, le coordinateur pour les services numériques de l'État membre d'établissement, ainsi que le comité et tout autre coordinateur pour les services numériques le cas échéant, devraient fournir à la Commission toutes les informations et l'assistance nécessaires pour lui permettre de s'acquitter efficacement de ses tâches, y compris les informations recueillies dans le cadre d'une collecte de données ou d'exercices d'accès aux données, dans la mesure où cela n'est pas interdit par la base juridique en vertu de laquelle les informations ont été recueillies. Réciproquement, la Commission devrait tenir le coordinateur pour les services numériques de l'État membre d'établissement et le comité informés de l'exercice de ses pouvoirs, en particulier lorsqu'elle a l'intention d'engager la procédure et d'exercer ses pouvoirs d'enquête. Par ailleurs, lorsque la Commission communique ses conclusions préliminaires, y compris toute question sur laquelle elle exprime des griefs, aux fournisseurs de très grandes plateformes en ligne ou de très grands moteurs de recherche en ligne concernés, elle devrait également les communiquer au comité. Le comité devrait faire connaître son point de vue sur les griefs et l'appréciation émis par la Commission, qui devrait prendre en compte cet avis dans la motivation sous-tendant sa décision définitive.

(140)

Compte tenu à la fois des difficultés particulières qui peuvent surgir dans le cadre de la vérification du respect des règles par les fournisseurs de très grandes plateformes en ligne ou de très grands moteurs de recherche en ligne et de l'importance de procéder efficacement à cette vérification, eu égard à leur taille, à leur poids et au préjudice qu'ils peuvent causer, la Commission devrait disposer de pouvoirs d'enquête et d'exécution solides pour lui permettre d'enquêter sur le respect des règles établies dans le présent règlement, de les faire appliquer et de contrôler leur respect, dans le plein respect du droit fondamental d'être entendu et d'avoir accès au dossier dans le cadre de procédures d'exécution, du principe de proportionnalité et des droits et intérêts des parties affectées.

(141)

La Commission devrait pouvoir demander les informations nécessaires aux fins de veiller à la mise en œuvre et au respect effectifs des obligations fixées dans le présent règlement, dans l'ensemble de l'Union. En particulier, la Commission devrait avoir accès à tous les documents, données et informations pertinents nécessaires pour ouvrir et mener des enquêtes et pour contrôler le respect des obligations pertinentes prévues par le présent règlement, quelle que soit la personne qui détient les documents, données ou informations en question, et quels que soient la forme ou le format de ceux-ci, leur support de stockage ou le lieu précis où ils sont stockés. La Commission devrait pouvoir exiger directement, au moyen d'une demande d'informations dûment motivée, que le fournisseur de la très grande plateforme en ligne ou du très grand moteur de recherche en ligne en cause, ainsi que toute autre personne physique ou morale agissant pour les besoins de leur activité commerciale, industrielle, artisanale ou libérale et raisonnablement susceptible d'avoir connaissance d'informations relatives à l'infraction présumée ou à l'infraction, selon le cas, fournisse tout élément de preuve, toute donnée et toute information pertinents. En outre, la Commission devrait pouvoir demander toute information pertinente à toute autorité publique, tout organisme ou toute agence au sein de l'État membre aux fins du présent règlement. La Commission devrait pouvoir exiger, par l'exercice de pouvoirs d'enquête, tels que des demandes d'informations ou des auditions, l'accès aux documents, aux données, aux informations, aux bases de données et aux algorithmes des personnes concernées ainsi que des explications y afférentes, interroger, avec son consentement, toute personne physique ou morale susceptible d'être en possession d'informations utiles et enregistrer les déclarations correspondantes par tout moyen technique. La Commission devrait également être habilitée à effectuer les inspections nécessaires pour faire respecter les dispositions pertinentes du présent règlement. Ces pouvoirs d'enquête visent à compléter la possibilité pour la Commission de demander l'assistance des coordinateurs pour les services numériques et des autorités d'autres États membres, par exemple par la fourniture d'informations ou dans l'exercice de ces pouvoirs.

(142)

Les mesures provisoires peuvent être un outil important pour s'assurer que, pendant qu'une enquête est en cours, l'infraction faisant l'objet de l'enquête n'entraîne pas de risque de préjudices graves pour les destinataires du service. Cet instrument joue un rôle important pour éviter une évolution qu'il serait très difficile d'inverser par une décision prise par la Commission à la fin de la procédure. La Commission devrait par conséquent avoir le pouvoir de décider d'imposer des mesures provisoires dans le cadre d'une procédure engagée en vue de l'adoption éventuelle d'une décision constatant un manquement. Ce pouvoir devrait s'appliquer dans les cas où la Commission a conclu à première vue à l'existence d'une violation d'obligations prévues au présent règlement par le fournisseur d'une très grande

plateforme en ligne ou d'un très grand moteur de recherche en ligne. Une décision imposant des mesures provisoires ne devrait s'appliquer que pour une durée déterminée, soit jusqu'au terme de la procédure engagée par la Commission, soit pour une période déterminée, qui peut être renouvelée dans la mesure où cela est nécessaire et opportun.

(143)

La Commission devrait pouvoir prendre les mesures nécessaires pour contrôler la mise en œuvre et le respect effectifs des obligations prévues par le présent règlement. Au titre de ces mesures, elle devrait avoir la capacité de nommer des experts externes indépendants et des auditeurs chargés de l'assister dans ce processus, y compris, le cas échéant, issus des autorités compétentes des États membres, par exemple les autorités chargées de la protection des données ou de la protection des consommateurs. Lors de la désignation des auditeurs, la Commission devrait veiller à une rotation suffisante.

(144)

Le non-respect des obligations pertinentes imposées en vertu du présent règlement devrait pouvoir être sanctionné au moyen d'amendes et d'astreintes. À cette fin, il convient également de fixer des niveaux appropriés d'amendes et d'astreintes en cas de non-respect des obligations et de violation des règles de procédure, sous réserve de délais de prescription appropriés conformément aux principes de proportionnalité et non bis in idem. La Commission et les autorités nationales compétentes devraient coordonner leurs efforts en matière d'exécution afin de veiller au respect desdits principes. En particulier, la Commission devrait tenir compte de toutes les amendes et astreintes imposées à la même personne morale pour les mêmes faits par une décision finale dans le cadre d'une procédure relative à une infraction à d'autres règles nationales ou de l'Union, de manière à veiller à ce que l'ensemble des amendes et astreintes imposées soient proportionnées et correspondent à la gravité des infractions commises. Toutes les décisions prises par la Commission au titre du présent règlement sont soumises au contrôle de la Cour de justice de l'Union européenne conformément au traité sur le fonctionnement de l'Union européenne. La Cour de justice de l'Union européenne devrait disposer d'une compétence de pleine juridiction en ce qui concerne les amendes et les astreintes conformément à l'article 261 du traité sur le fonctionnement de l'Union européenne.

(145)

Eu égard aux effets potentiellement importants pour la société que peut avoir une violation des obligations supplémentaires de gestion des risques systémiques qui s'appliquent exclusivement aux très grandes plateformes en ligne et aux très grands moteurs de recherche en ligne, et afin de répondre à ces préoccupations de politique publique, il est nécessaire de prévoir un système de surveillance renforcée de toute mesure prise pour mettre fin efficacement aux violations du présent règlement et pour y remédier. Par conséquent, dès qu'une infraction à l'une des dispositions du présent règlement qui s'appliquent exclusivement aux très grandes plateformes en ligne ou aux très grands moteurs de recherche en ligne a été constatée et, s'il y a lieu, sanctionnée, la Commission devrait demander au fournisseur de la plateforme ou du moteur de recherche en cause d'établir un plan d'action détaillé pour remédier à tout effet futur de l'infraction et de communiquer ce plan d'action, dans un délai fixé par la Commission, aux coordinateurs pour les services numériques, à la Commission et au comité. La Commission, tenant compte de l'avis du comité, devrait

déterminer si les mesures prévues dans le plan d'action sont suffisantes pour remédier à l'infraction, en prenant également en considération le fait que l'adhésion au code de conduite pertinent figure ou non parmi les mesures proposées. La Commission devrait en outre vérifier toute mesure ultérieure prise par le fournisseur de la très grande plateforme en ligne ou du très grand moteur de recherche en ligne en cause conformément à son plan d'action, en tenant compte aussi d'un audit indépendant du fournisseur. Si, à la suite de la mise en œuvre du plan d'action, la Commission considère toujours qu'il n'a pas été pleinement remédié à l'infraction, ou si le plan d'action n'a pas été fourni ou n'est pas considéré comme adéquat, elle devrait pouvoir utiliser tout pouvoir d'enquête ou d'exécution prévu par le présent règlement, y compris le pouvoir d'imposer des astreintes et l'ouverture d'une procédure visant à rendre impossible l'accès au service fourni en violation du présent règlement.

(146)

Il convient que le fournisseur de la très grande plateforme en ligne ou du très grand moteur de recherche en ligne en cause ainsi que les autres personnes soumises à l'exercice des pouvoirs de la Commission dont les intérêts peuvent être affectés par une décision, aient la possibilité de présenter leurs observations au préalable, et une large publicité des décisions prises devrait être assurée. Tout en garantissant les droits de la défense des parties concernées, et notamment le droit d'accès au dossier, il est indispensable de préserver la confidentialité des informations. En outre, tout en respectant la confidentialité des informations, la Commission devrait veiller à ce que toute information invoquée aux fins de sa décision soit divulguée dans une mesure permettant au destinataire de la décision de comprendre les faits et considérations qui ont conduit à celle-ci.

(147)

Afin de garantir que le présent règlement est appliqué et exécuté de façon harmonisée, il importe de veiller à ce que les autorités nationales, y compris les juridictions nationales, disposent de toutes les informations nécessaires pour garantir que leurs décisions ne soient pas contraires à une décision adoptée par la Commission en vertu du présent règlement. Cette disposition est sans préjudice de l'article 267 du traité sur le fonctionnement de l'Union européenne.

(148)

L'exécution et le contrôle effectifs du présent règlement nécessitent un échange d'informations fluide et en temps réel entre les coordinateurs pour les services numériques, le comité et la Commission, sur la base des flux d'informations et des procédures prévus dans le présent règlement. Cela peut également justifier, s'il y a lieu, l'accès à ce système par d'autres autorités compétentes. Dans le même temps, compte tenu du fait que les informations échangées peuvent être confidentielles ou comporter des données à caractère personnel, elles devraient rester protégées contre tout accès non autorisé, conformément aux finalités pour lesquelles elles ont été recueillies. Pour cette raison, toutes les communications entre ces autorités devraient avoir lieu sur la base d'un système de partage d'informations fiable et sécurisé, dont les détails devraient être fixés dans un acte d'exécution. Le système de partage d'informations peut être fondé sur des outils existants du marché intérieur, dans la mesure où ceux-ci permettent d'atteindre les objectifs du présent règlement de manière économiquement avantageuse.

(149)

Sans préjudice du droit des destinataires de services de s'adresser à un représentant conformément à la directive (UE) 2020/1828 du Parlement européen et du Conseil (33) ou à tout autre type de représentation au titre du droit national, les destinataires des services devraient également avoir le droit de mandater une personne morale ou un organisme public pour exercer les droits qui leur sont conférés par le présent règlement. Ces droits peuvent inclure les droits liés à la soumission de notifications, à la contestation des décisions prises par les fournisseurs de services intermédiaires et à l'introduction de plaintes contre les fournisseurs pour violation du présent règlement. Certains organismes, organisations et associations disposent d'une expertise et de compétences particulières pour la détection et le signalement des décisions relatives à la modération des contenus erronées ou injustifiés et les réclamations qu'ils adressent au nom des destinataires du service peuvent avoir un impact positif sur la liberté d'expression et d'information en général; par conséquent, les fournisseurs de plateformes en ligne devraient traiter ces réclamations sans retard injustifié.

(150)

Dans un souci d'efficacité et d'efficience, la Commission devrait procéder à une évaluation générale du présent règlement. En particulier, cette évaluation générale devrait, entre autres, porter sur l'étendue des services couverts par le présent règlement, les interactions avec d'autres actes juridiques, l'impact du présent règlement sur le fonctionnement du marché intérieur, notamment en ce qui concerne les services numériques, la mise en œuvre des codes de conduite, l'obligation de désigner un représentant légal établi dans l'Union, l'effet des obligations sur les petites entreprises et les microentreprises, l'efficacité du mécanisme de surveillance de d'exécution et l'impact sur le droit à la liberté d'expression et d'information. En outre, afin d'éviter des charges disproportionnées et de garantir le maintien de l'efficacité du présent règlement, la Commission devrait procéder à une évaluation de l'impact des obligations énoncées dans le présent règlement sur les petites et moyennes entreprises dans les trois ans à compter du début de son application ainsi qu'à une évaluation de l'étendue des services couverts par le présent règlement, notamment pour les très grandes plateformes en ligne et les très grands moteurs de recherche, et les interactions avec d'autres actes juridiques dans les trois ans à compter de son entrée en vigueur.

(151)

Afin d'assurer des conditions uniformes d'exécution du présent règlement, il convient de conférer des compétences d'exécution à la Commission pour établir des modèles concernant la forme, le contenu et d'autres détails des rapports sur la modération des contenus, établir le montant de la redevance de surveillance annuelle imposée aux fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne, fixer les modalités pratiques des procédures, des auditions et de la divulgation négociée d'informations effectuées dans le cadre de la surveillance, des enquêtes, de l'exécution et du contrôle à l'égard des fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne, ainsi que pour fixer les modalités pratiques et opérationnelles du fonctionnement du système de partage d'informations et de son interopérabilité avec d'autres systèmes pertinents. Ces compétences devraient être exercées conformément au règlement (UE) n° 182/2011 du Parlement européen et du Conseil (34).

(152)

Afin de réaliser les objectifs du présent règlement, il convient de déléguer à la Commission le pouvoir d'adopter des actes conformément à l'article 290 du traité sur le fonctionnement de l'Union européenne pour compléter ledit règlement en ce qui concerne les critères d'identification des très grandes plateformes en ligne et des très grands moteurs de recherche en ligne, les étapes procédurales, les méthodologies et les modèles de rapport pour les audits, les spécifications techniques des demandes d'accès ainsi que la méthodologie et les procédures détaillées pour fixer la redevance de surveillance. Il importe particulièrement que la Commission procède aux consultations appropriées durant son travail préparatoire, y compris au niveau des experts, et que ces consultations soient menées conformément aux principes définis dans l'accord interinstitutionnel du 13 avril 2016"Mieux légiférer" (35). En particulier, pour assurer leur égale participation à la préparation des actes délégués, le Parlement européen et le Conseil reçoivent tous les documents au même moment que les experts des États membres, et leurs experts ont systématiquement accès aux réunions des groupes d'experts de la Commission traitant de la préparation des actes délégués.

(153)

Le présent règlement respecte les droits fondamentaux reconnus par la Charte et les droits fondamentaux qui constituent des principes généraux du droit de l'Union. Par conséquent, il convient d'interpréter le présent règlement et de l'appliquer conformément à ces droits fondamentaux, y compris la liberté d'expression et d'information et la liberté et le pluralisme des médias. Dans l'exercice des pouvoirs énoncés dans le présent règlement, toute autorité publique concernée devrait parvenir, dans les situations où les droits fondamentaux pertinents entrent en conflit, à un juste équilibre entre les droits concernés, conformément au principe de proportionnalité.

(154)

Compte tenu de la portée et de l'incidence des risques pour la société pouvant être causés par les très grandes plateformes en ligne et les très grands moteurs de recherche en ligne, de la nécessité de répondre à ces risques de manière prioritaire et de la capacité à prendre les mesures nécessaires, il est justifié de limiter la période après laquelle le présent règlement commence à s'appliquer aux fournisseurs de ces services.

(155)

Étant donné que les objectifs du présent règlement, à savoir contribuer au bon fonctionnement du marché intérieur et garantir un environnement en ligne sûr, prévisible et fiable dans lequel les droits fondamentaux consacrés par la Charte sont dûment protégés, ne peuvent pas être atteints de manière suffisante par les États membres en raison de l'impossibilité d'assurer l'harmonisation et la coopération nécessaires en agissant de manière isolée, mais peuvent, en raison du champ d'application territorial et personnel, l'être mieux au niveau de l'Union, celle-ci peut prendre des mesures, conformément au principe de subsidiarité consacré à l'article 5 du traité sur l'Union européenne. Conformément au principe de proportionnalité énoncé audit article, le présent règlement n'excède pas ce qui est nécessaire pour atteindre ces objectifs.

(156)

Le Contrôleur européen de la protection des données a été consulté conformément à l'article 42, paragraphe 1, du règlement (UE) 2018/1725 du Parlement européen et du Conseil (36) et a rendu son avis le 10 février 2021 (37),

ONT ADOPTÉ LE PRÉSENT RÈGLEMENT :

CHAPITRE I

DISPOSITIONS GÉNÉRALES

Article premier

Objet

1. Le présent règlement a pour objectif de contribuer au bon fonctionnement du marché intérieur des services intermédiaires en établissant des règles harmonisées pour un environnement en ligne sûr, prévisible et fiable qui facilite l'innovation et dans lequel les droits fondamentaux consacrés par la Charte, y compris le principe de protection des consommateurs, sont efficacement protégés.

2. Le présent règlement établit des règles harmonisées applicables à la fourniture de services intermédiaires au sein du marché intérieur. En particulier, il établit:

a)

un cadre pour l'exemption conditionnelle de responsabilité des fournisseurs de services intermédiaires;

b)

des règles relatives à des obligations de diligence spécifiques, adaptées à certaines catégories spécifiques de fournisseurs de services intermédiaires;

c)

des règles relatives à la mise en œuvre et à l'exécution du présent règlement, y compris en ce qui concerne la coopération et la coordination entre les autorités compétentes.

Article 2

Champ d'application

1. Le présent règlement s'applique aux services intermédiaires proposés aux destinataires du service dont le lieu d'établissement est situé dans l'Union ou qui sont situés dans l'Union, quel que soit le lieu d'établissement des fournisseurs de ces services intermédiaires.

2. Le présent règlement ne s'applique pas aux services qui ne sont pas des services intermédiaires ou aux exigences imposées à l'égard de tels services, que ces services soient ou non fournis par le biais d'un service intermédiaire.

3. Le présent règlement n'a pas d'incidence sur l'application de la directive 2000/31/CE.

4. Le présent règlement s'entend sans préjudice des règles établies par d'autres actes juridiques de l'Union régissant d'autres aspects de la fourniture de services intermédiaires dans le marché intérieur ou précisant et complétant le présent règlement, en particulier les actes suivants:

a) la directive 2010/13/UE;

b) le droit de l'Union sur le droit d'auteur et les droits voisins;

c) le règlement (UE) 2021/784;

d) le règlement (UE) 2019/1148;

e) le règlement (UE) 2019/1150;

f) le droit de l'Union en matière de protection des consommateurs et de sécurité des produits, notamment les règlements (UE) 2017/2394 et (UE) 2019/1020 et les directives 2001/95/CE et 2013/11/UE;

g) le droit de l'Union en matière de protection des données à caractère personnel, en particulier le règlement (UE) 2016/679 et la directive 2002/58/CE;

h) le droit de l'Union dans le domaine de la coopération judiciaire en matière civile, en particulier le règlement (UE) n° 1215/2012 ou tout acte juridique de l'Union fixant les règles relatives à la loi applicable aux obligations contractuelles et non contractuelles;

i) le droit de l'Union dans le domaine de la coopération judiciaire en matière pénale, en particulier un règlement relatif aux injonctions européennes de production et de conservation de preuves électroniques en matière pénale;

j) une directive établissant des règles harmonisées concernant la désignation de représentants légaux aux fins de la collecte de preuves en matière pénale.

Article 3

Définitions

Aux fins du présent règlement, on entend par:

a) "service de la société de l'information": un service tel qu'il est défini à l'article 1er, paragraphe 1, point b), de la directive (UE) 2015/1535;

b) "destinataire du service": toute personne physique ou morale utilisant un service intermédiaire, notamment pour rechercher une information ou la rendre accessible;

c) "consommateur": toute personne physique agissant à des fins qui n'entrent pas dans le cadre de son activité commerciale, industrielle, artisanale ou libérale;

d) “proposer des services dans l’Union”: permettre aux personnes physiques ou morales dans un ou plusieurs États membres d’utiliser les services d’un fournisseur de services intermédiaires qui a un lien étroit avec l’Union;

e) “lien étroit avec l’Union”: un lien qu’un fournisseur de services intermédiaires a avec l’Union résultant soit de son établissement dans l’Union, soit de critères factuels spécifiques, tels que:

- un nombre significatif de destinataires du service dans un ou plusieurs États membres par rapport à sa ou à leur population; ou

- le ciblage des activités sur un ou plusieurs États membres;

f) “professionnel”: toute personne physique, ou toute personne morale qu’elle soit privée ou publique, qui agit, y compris par l’intermédiaire d’une personne agissant en son nom ou pour son compte, à des fins entrant dans le cadre de son activité commerciale, industrielle, artisanale ou libérale;

g) “service intermédiaire”: un des services de la société de l’information suivants:

h) un service de “simple transport”, consistant à transmettre, sur un réseau de communication, des informations fournies par un destinataire du service ou à fournir l’accès à un réseau de communication;

ii) un service de “mise en cache”, consistant à transmettre, sur un réseau de communication, des informations fournies par un destinataire du service, impliquant le stockage automatique, intermédiaire et temporaire de ces informations, effectué dans le seul but de rendre plus efficace la transmission ultérieure de ces informations à d’autres destinataires à leur demande;

iii) un service d’”hébergement”, consistant à stocker des informations fournies par un destinataire du service à sa demande;

i) “contenu illicite”: toute information qui, en soi ou par rapport à une activité, y compris la vente de produits ou la fourniture de services, n’est pas conforme au droit de l’Union ou au droit d’un État membre qui est conforme au droit de l’Union, quel que soit l’objet précis ou la nature précise de ce droit;

j) “plateforme en ligne”: un service d’hébergement qui, à la demande d’un destinataire du service, stocke et diffuse au public des informations, à moins que cette activité ne soit une caractéristique mineure et purement accessoire d’un autre service ou une fonctionnalité mineure du service principal qui, pour des raisons objectives et techniques, ne peut être utilisée sans cet autre service, et pour autant que l’intégration de cette caractéristique ou de cette fonctionnalité à l’autre service ne soit pas un moyen de contourner l’applicabilité du présent règlement;

k) “moteur de recherche en ligne”: un service intermédiaire qui permet aux utilisateurs de formuler des requêtes afin d’effectuer des recherches sur, en principe, tous les sites internet ou tous les sites internet dans une langue donnée, sur la base d’une requête lancée sur n’importe quel sujet sous la forme d’un mot-clé, d’une demande vocale,

d'une expression ou d'une autre entrée, et qui renvoie des résultats dans quelque format que ce soit dans lesquels il est possible de trouver des informations en rapport avec le contenu demandé;

l) "diffusion au public": le fait de mettre des informations à la disposition d'un nombre potentiellement illimité de tiers, à la demande du destinataire du service ayant fourni ces informations;

m) "contrat à distance": le "contrat à distance" tel qu'il est défini à l'article 2, point 7), de la directive 2011/83/UE;

n) "interface en ligne": tout logiciel, y compris un site internet ou une section de site internet, et des applications, notamment des applications mobiles;

o) "coordinateur pour les services numériques de l'État membre d'établissement": le coordinateur pour les services numériques de l'État membre dans lequel l'établissement principal d'un fournisseur d'un service intermédiaire est situé, ou dans lequel son représentant légal réside ou est établi;

p) "coordinateur pour les services numériques de l'État membre de destination": le coordinateur pour les services numériques d'un État membre dans lequel le service intermédiaire est fourni;

q) "destinataire actif d'une plateforme en ligne": un destinataire du service qui a été en contact avec une plateforme en ligne, soit en demandant à la plateforme en ligne d'héberger des informations, soit en étant exposé aux informations hébergées par la plateforme en ligne et diffusées via son interface en ligne;

r) "destinataire actif d'un moteur de recherche en ligne": un destinataire du service qui a soumis une requête à un moteur de recherche en ligne et a été exposé aux informations indexées et présentées sur son interface en ligne;

s) "publicité": les informations destinées à promouvoir le message d'une personne physique ou morale, qu'elles aient des visées commerciales ou non commerciales, et présentées par une plateforme en ligne sur son interface en ligne, moyennant rémunération, dans le but spécifique de promouvoir ces informations;

t) "système de recommandation": un système entièrement ou partiellement automatisé utilisé par une plateforme en ligne pour suggérer sur son interface en ligne des informations spécifiques aux destinataires du service ou pour hiérarchiser ces informations, notamment à la suite d'une recherche lancée par le destinataire du service ou en déterminant de toute autre manière l'ordre relatif ou d'importance des informations affichées;

u) "modération des contenus": les activités, qu'elles soient automatisées ou non, entreprises par des fournisseurs de services intermédiaires qui sont destinées, en particulier, à détecter et à identifier les contenus illicites ou les informations incompatibles avec leurs conditions générales, fournis par les destinataires du service, et à lutter contre ces contenus ou ces informations, y compris les mesures prises qui ont une incidence sur la disponibilité, la visibilité et l'accessibilité de ces contenus ou ces informations, telles que leur rétrogradation, leur démonétisation, le fait de rendre

l’accès à ceux-ci impossible ou leur retrait, ou qui ont une incidence sur la capacité des destinataires du service à fournir ces informations, telles que la suppression ou la suspension du compte d’un destinataire;

v) “conditions générales”: toutes les clauses, quelle que soit leur dénomination ou leur forme, qui régissent la relation contractuelle entre le fournisseur de services intermédiaires et les destinataires du service;

w) “personnes handicapées”: les “personnes handicapées” visées à l’article 3, point 1), de la directive (UE) 2019/882 du Parlement européen et du Conseil (38);

x) “communication commerciale”: la “communication commerciale” telle qu’elle est définie à l’article 2, point f), de la directive 2000/31/CE;

y) “chiffre d’affaires”: le montant atteint par une entreprise au sens de l’article 5, paragraphe 1, du règlement (CE) n° 139/2004 du Conseil (39).

CHAPITRE II

RESPONSABILITE DES FOURNISSEURS DE SERVICES INTERMÉDIAIRES

article 4 “Simple transport”

1. En cas de fourniture d’un service de la société de l’information consistant à transmettre, sur un réseau de communication, des informations fournies par un destinataire du service ou à fournir un accès à un réseau de communication, le fournisseur de services n’est pas responsable des informations transmises ou auxquelles l’accès est fourni, à condition que le fournisseur:

a) ne soit pas à l’origine de la transmission;

b) ne sélectionne pas le destinataire de la transmission; et

c) ne sélectionne et ne modifie pas les informations faisant l’objet de la transmission.

2. Les activités de transmission et de fourniture d’accès visées au paragraphe 1 englobent le stockage automatique, intermédiaire et transitoire des informations transmises, pour autant que ce stockage serve exclusivement à l’exécution de la transmission sur le réseau de communication et que sa durée n’excède pas le temps raisonnablement nécessaire à la transmission.

3. Le présent article n’affecte pas la possibilité, pour une autorité judiciaire ou administrative, conformément au système juridique d’un État membre, d’exiger du fournisseur de services qu’il mette fin à une infraction ou qu’il prévienne une infraction.

Article 5 - “Mise en cache”

1. En cas de fourniture d’un service de la société de l’information consistant à transmettre, sur un réseau de communication, des informations fournies par un destinataire du service, le

fournisseur de services n'est pas responsable du stockage automatique, intermédiaire et temporaire de ces informations réalisé dans le seul but de rendre plus efficace ou plus sûre la transmission ultérieure des informations à d'autres destinataires du service à leur demande, à condition que le fournisseur:

a) ne modifie pas les informations;

b) respecte les conditions d'accès aux informations;

c) respecte les règles concernant la mise à jour des informations, indiquées d'une manière largement reconnue et utilisées par le secteur;

d) n'entrave pas l'utilisation licite de la technologie, largement reconnue et utilisée par le secteur, dans le but d'obtenir des données sur l'utilisation des informations; et

e) agisse promptement pour retirer les informations qu'il a stockées ou pour rendre l'accès à ces informations impossible dès qu'il a effectivement connaissance du fait que les informations à l'origine de la transmission ont été retirées du réseau ou que l'accès aux informations a été rendu impossible, ou du fait qu'une autorité judiciaire ou administrative a ordonné de retirer les informations ou de rendre l'accès à ces informations impossible.

2. Le présent article n'affecte pas la possibilité, pour une autorité judiciaire ou administrative, conformément au système juridique d'un État membre, d'exiger du fournisseur de services qu'il mette fin à une infraction ou qu'il prévienne une infraction.

Article 6 - Hébergement

1. En cas de fourniture d'un service de la société de l'information consistant à stocker des informations fournies par un destinataire du service, le fournisseur de services n'est pas responsable des informations stockées à la demande d'un destinataire du service à condition que le fournisseur:

a) n'ait pas effectivement connaissance de l'activité illégale ou du contenu illicite et, en ce qui concerne une demande en dommages et intérêts, n'ait pas conscience de faits ou de circonstances selon lesquels l'activité illégale ou le contenu illicite est apparent; ou

b) dès le moment où il en prend connaissance ou conscience, agisse promptement pour retirer le contenu illicite ou rendre l'accès à celui-ci impossible.

2. Le paragraphe 1 ne s'applique pas lorsque le destinataire du service agit sous l'autorité ou le contrôle du fournisseur.

3. Le paragraphe 1 ne s'applique pas en ce qui concerne la responsabilité au titre de la législation relative à la protection des consommateurs applicable aux plateformes en ligne permettant aux consommateurs de conclure des contrats à distance avec des professionnels, lorsqu'une telle plateforme en ligne présente l'information spécifique ou permet de toute autre manière la transaction spécifique en question de telle sorte qu'un consommateur moyen peut être amené à croire que les informations, le produit ou service faisant l'objet de la transaction

sont fournis soit directement par la plateforme en ligne, soit par un destinataire du service agissant sous son autorité ou son contrôle.

4. Le présent article n'affecte pas la possibilité, pour une autorité judiciaire ou administrative, conformément au système juridique d'un État membre, d'exiger du fournisseur de services qu'il mette fin à une infraction ou qu'il prévienne une infraction.

Article 7- Enquêtes d'initiative volontaires et respect de la législation

Les fournisseurs de services intermédiaires ne sont pas réputés avoir droit aux exemptions de responsabilité prévues aux articles 4, 5 et 6 du simple fait qu'ils procèdent de leur propre initiative, de bonne foi et avec diligence, à des enquêtes volontaires ou prennent d'autres mesures destinées à détecter, à identifier et à retirer des contenus illicites, ou à rendre l'accès à ces contenus impossible, ou qu'ils prennent les mesures nécessaires pour se conformer aux exigences du droit de l'Union et du droit national conforme au droit de l'Union, y compris les exigences énoncées dans le présent règlement.

Article 8- Absence d'obligation générale de surveillance ou de recherche active des faits

Les fournisseurs de services intermédiaires ne sont soumis à aucune obligation générale de surveiller les informations qu'ils transmettent ou stockent ou de rechercher activement des faits ou des circonstances révélant des activités illégales.

Article 9- Injonctions d'agir contre des contenus illicites

1. Dès réception d'une injonction d'agir contre un ou plusieurs éléments spécifiques de contenu illicite, émise par les autorités judiciaires ou administratives nationales compétentes sur la base du droit de l'Union ou du droit national conforme au droit de l'Union applicable, le fournisseur de services intermédiaires informe dans les meilleurs délais l'autorité qui a émis l'injonction, ou toute autre autorité spécifiée dans l'injonction, de la suite éventuelle donnée à l'injonction, en précisant si et quand une suite a été donnée à l'injonction.

2. Lorsqu'une injonction visée au paragraphe 1 est transmise au fournisseur, les États membres veillent à ce qu'elle remplisse au minimum les conditions suivantes:

a) ladite injonction comprend les éléments suivants:

i) une référence à la base juridique au titre du droit de l'Union ou du droit national pour l'injonction;

ii) un exposé des motifs expliquant pourquoi les informations constituent un contenu illicite, en référence à une ou plusieurs dispositions spécifiques du droit de l'Union ou du droit national conforme au droit de l'Union;

iii) des informations permettant d'identifier l'autorité d'émission;

iv) des informations claires permettant au fournisseur de services intermédiaires d'identifier et de localiser le contenu illicite concerné, telles qu'un ou plusieurs URL exacts et, si nécessaire, des informations supplémentaires;

v) des informations relatives aux mécanismes de recours dont disposent le fournisseur de services intermédiaires et le destinataire du service ayant fourni le contenu;

vi) le cas échéant, des informations sur l'autorité qui doit recevoir les informations relatives aux suites données aux injonctions;

b) le champ d'application territorial de ladite injonction, sur la base des règles applicables du droit de l'Union et du droit national, y compris de la Charte, et, le cas échéant, des principes généraux du droit international, est limité à ce qui est strictement nécessaire pour atteindre son objectif;

c) ladite injonction est transmise dans l'une des langues déclarées par le fournisseur de services intermédiaires en vertu de l'article 11, paragraphe 3, ou dans une autre langue officielle des États membres convenue entre l'autorité qui a émis l'injonction et ce fournisseur, et elle est envoyée au point de contact électronique désigné par ce fournisseur, conformément à l'article 11; lorsque l'injonction n'est pas rédigée dans la langue déclarée par le fournisseur de services intermédiaires ou dans une autre langue convenue de manière bilatérale, l'injonction peut être transmise dans la langue de l'autorité qui l'a émise, à condition qu'elle soit accompagnée d'une traduction, dans la langue déclarée ou convenue de manière bilatérale, au minimum des éléments mentionnés aux points a) et b) du présent paragraphe.

3. L'autorité qui a émis l'injonction ou, le cas échéant, l'autorité spécifiée dans l'injonction, transmet l'injonction ainsi que toute information reçue du fournisseur de services intermédiaires concernant la suite donnée à cette injonction au coordinateur pour les services numériques de l'État membre de l'autorité d'émission.

4. Après avoir reçu l'injonction de l'autorité judiciaire ou administrative, le coordinateur pour les services numériques de l'État membre concerné transmet, dans les meilleurs délais, une copie de l'injonction visée au paragraphe 1 du présent article à tous les autres coordinateurs pour les services numériques par l'intermédiaire du système établi conformément à l'article 85.

5. Au plus tard lorsqu'une suite est donnée à l'injonction ou, le cas échéant, au moment indiqué par l'autorité d'émission dans son injonction, les fournisseurs de services intermédiaires informent le destinataire du service concerné de l'injonction reçue et de la suite qui lui est donnée. Les informations communiquées au destinataire du service comprennent un exposé des motifs, les possibilités de recours qui existent et une description du champ d'application territorial de l'injonction, conformément au paragraphe 2.

6. Les conditions et exigences établies dans le présent article sont sans préjudice du droit national applicable en matière de procédure civile et de procédure pénale.

Article 10 - Injonctions de fournir des informations

1. Dès réception de l'injonction de fournir des informations spécifiques concernant un ou plusieurs destinataires spécifiques du service, émise par les autorités judiciaires ou administratives nationales compétentes sur la base du droit de l'Union ou du droit national conforme au droit de l'Union applicable, le fournisseur de services intermédiaires informe,

dans les meilleurs délais, l'autorité qui a émis l'injonction, ou toute autre autorité spécifiée dans l'injonction, de la réception de l'injonction et de la suite qui y est donnée, en précisant si et quand une suite a été donnée à l'injonction.

2. Lorsqu'une injonction visée au paragraphe 1 est transmise au fournisseur, les États membres veillent à ce qu'elle remplisse au minimum les conditions suivantes:

a) ladite injonction comprend les éléments suivants:

   i) une référence à la base juridique au titre du droit de l'Union ou du droit national pour l'injonction;

   ii) des informations permettant d'identifier l'autorité d'émission;

   iii) des informations claires permettant au fournisseur de services intermédiaires d'identifier le ou les destinataires spécifiques au sujet desquels des informations sont demandées, telles qu'un ou plusieurs noms de compte ou identifiants uniques;

   iv) un exposé des motifs expliquant dans quel but les informations sont requises et pourquoi la demande de fourniture d'informations est nécessaire et proportionnée pour déterminer si les destinataires des services intermédiaires respectent le droit de l'Union ou le droit national conforme au droit de l'Union applicable, à moins qu'un tel exposé ne puisse être fourni pour des raisons liées à la prévention et à la détection des infractions pénales et aux enquêtes et poursuites en la matière;

   v) des informations relatives aux mécanismes de recours dont disposent le fournisseur et les destinataires du service concerné;

   vi) le cas échéant, des informations relatives à l'autorité qui doit recevoir les informations relatives aux suites données aux injonctions;

b) ladite injonction exige uniquement du fournisseur qu'il communique des informations déjà collectées aux fins de fournir le service et dont il a le contrôle;

c) ladite injonction est transmise dans l'une des langues déclarées par le fournisseur de services intermédiaires en vertu de l'article 11, paragraphe 3, ou dans une autre langue officielle des États membres convenue entre l'autorité qui a émis l'injonction et le fournisseur, et elle est envoyée au point de contact électronique désigné par ce fournisseur, conformément à l'article 11; lorsque l'injonction n'est pas rédigée dans la langue déclarée par le fournisseur de services intermédiaires ou dans une autre langue convenue de manière bilatérale, l'injonction peut être transmise dans la langue de l'autorité qui l'a émise, à condition qu'elle soit accompagnée d'une traduction, dans cette langue déclarée ou convenue de manière bilatérale, au minimum des éléments mentionnés aux points a) et b) du présent paragraphe.

3. L'autorité qui a émis l'injonction ou, le cas échéant, l'autorité spécifiée dans l'injonction, transmet l'injonction ainsi que toute information reçue du fournisseur de services

intermédiaires concernant la suite donnée à cette injonction au coordinateur pour les services numériques de l'État membre de l'autorité d'émission.

4. Après avoir reçu l'injonction de l'autorité judiciaire ou administrative, le coordinateur pour les services numériques de l'État membre concerné transmet, dans les meilleurs délais, une copie de l'injonction visée au paragraphe 1 du présent article à tous les coordinateurs pour les services numériques par l'intermédiaire du système établi conformément à l'article 85.

5. Au plus tard lorsqu'une suite est donnée à l'injonction ou, le cas échéant, au moment indiqué par l'autorité d'émission dans son injonction, les fournisseurs de services intermédiaires informent le destinataire du service concerné de l'injonction reçue et de la suite qui lui est donnée. Les informations communiquées au destinataire du service comprennent un exposé des motifs et les possibilités de recours qui existent, conformément au paragraphe 2.

6. Les conditions et exigences énoncées dans le présent article sont sans préjudice du droit national applicable en matière de procédure civile et de procédure pénale.

CHAPITRE III

OBLIGATIONS DE DILIGENCE POUR UN ENVIRONNEMENT EN LIGNE SÛR ET TRANSPARENT

SECTION 1

Dispositions applicables à tous les fournisseurs de services intermédiaires

Article 11

Points de contact pour les autorités des États membres, la Commission et le comité

1. Les fournisseurs de services intermédiaires désignent un point de contact unique pour leur permettre de communiquer directement, par voie électronique, avec les autorités des États membres, la Commission et le comité visé à l'article 61 en vue de l'application du présent règlement.

2. Les fournisseurs de services intermédiaires rendent publiques les informations nécessaires pour faciliter l'identification de leurs points de contact uniques et la communication avec ces derniers. Ces informations sont aisément accessibles et sont tenues à jour.

3. Les fournisseurs de services intermédiaires précisent, dans les informations visées au paragraphe 2, la ou les langues officielles des États membres qui, en plus d'une langue largement comprise par le plus grand nombre possible de citoyens de l'Union, peuvent être utilisées pour communiquer avec leurs points de contact, et qui comprennent au minimum une des langues officielles de l'État membre dans lequel le fournisseur de services intermédiaires a son établissement principal ou dans lequel son représentant légal réside ou est établi.

Article 12

Points de contact pour les destinataires du service

1. Les fournisseurs de services intermédiaires désignent un point de contact unique pour permettre aux destinataires du service de communiquer directement et rapidement avec eux, par voie électronique et de manière conviviale, y compris en permettant aux destinataires du service de choisir les moyens de communication, lesquels ne s'appuient pas uniquement sur des outils automatisés.

2. Outre les obligations prévues dans la directive 2000/31/CE, les fournisseurs de services intermédiaires rendent publiques les informations nécessaires pour que les destinataires du service puissent facilement identifier leurs points de contact uniques et communiquer avec eux. Ces informations sont aisément accessibles et sont tenues à jour.

Article 13

Représentants légaux

1. Les fournisseurs de services intermédiaires qui n'ont pas d'établissement au sein de l'Union, mais qui proposent des services dans l'Union désignent, par écrit, une personne morale ou physique pour agir comme leur représentant légal dans un des États membres dans lequel le fournisseur propose ses services.

2. Les représentants légaux sont chargés par les fournisseurs de services intermédiaires de répondre, en sus ou à la place de ces fournisseurs, à toutes les questions des autorités compétentes des États membres, de la Commission et du comité nécessaires en vue de la réception, du respect et de l'exécution des décisions prises en lien avec le présent règlement. Les fournisseurs de services intermédiaires donnent à leur représentant légal les pouvoirs nécessaires et les ressources suffisantes pour garantir une coopération efficace et en temps utile avec les autorités compétentes des États membres, la Commission et le comité, et pour se conformer à ces décisions.

3. Le représentant légal désigné peut être tenu pour responsable du non-respect des obligations prévues dans le présent règlement, sans préjudice de la responsabilité du fournisseur de services intermédiaires et des actions en justice qui pourraient être intentées contre lui.

4. Les fournisseurs de services intermédiaires communiquent le nom, l'adresse postale, l'adresse de courrier électronique et le numéro de téléphone de leur représentant légal au coordinateur pour les services numériques de l'État membre dans lequel le représentant légal réside ou est établi. Ils veillent à ce que ces informations soient mises à la disposition du public, facilement accessibles, exactes et tenues à jour.

5. La désignation d'un représentant légal au sein de l'Union en vertu du paragraphe 1 ne constitue pas un établissement dans l'Union.

Article 14 - Conditions générales

1. Les fournisseurs de services intermédiaires incluent dans leurs conditions générales des renseignements relatifs aux éventuelles restrictions qu'ils imposent en ce qui concerne l'utilisation de leur service vis-à-vis des informations fournies par les destinataires du service. Ces renseignements comprennent des informations sur les politiques, procédures, mesures et

outils utilisés à des fins de modération des contenus, y compris la prise de décision fondée sur des algorithmes et le réexamen par un être humain, ainsi que sur le règlement intérieur de leur système interne de traitement des réclamations. Ils sont énoncés dans un langage clair, simple, intelligible, aisément abordable et dépourvu d'ambiguïté, et sont mis à la disposition du public dans un format facilement accessible et lisible par une machine.

2. Les fournisseurs de services intermédiaires informent les destinataires du service de toute modification importante des conditions générales.

3. Lorsqu'un service intermédiaire s'adresse principalement à des mineurs ou est utilisé de manière prédominante par des mineurs, le fournisseur de ce service intermédiaire explique les conditions et les éventuelles restrictions relatives à l'utilisation du service d'une manière compréhensible pour les mineurs.

4. Lorsqu'ils appliquent et font respecter les restrictions visées au paragraphe 1, les fournisseurs de services intermédiaires agissent de manière diligente, objective et proportionnée en tenant dûment compte des droits et des intérêts légitimes de toutes les parties impliquées, et notamment des droits fondamentaux des destinataires du service, tels que la liberté d'expression, la liberté et le pluralisme des médias et d'autres libertés et droits fondamentaux tels qu'ils sont consacrés dans la Charte.

5. Les fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne fournissent aux destinataires des services un résumé des conditions générales, y compris des mécanismes de recours et de réparation disponibles, concis, facilement accessible et lisible par une machine, dans un langage clair et dépourvu d'ambiguïté.

6. Les très grandes plateformes en ligne et les très grands moteurs de recherche en ligne au sens de l'article 33 publient leurs conditions générales dans les langues officielles de tous les États membres dans lesquels ils proposent leurs services.

Article 15- Obligations en matière de rapports de transparence incombant aux fournisseurs de services intermédiaires

1. Les fournisseurs de services intermédiaires mettent à la disposition du public, dans un format lisible par une machine et d'une manière facilement accessible, au moins une fois par an, des rapports clairs et facilement compréhensibles sur les éventuelles activités de modération des contenus auxquelles ils se sont livrés au cours de la période concernée. Ces rapports comprennent, en particulier, des informations sur les points suivants, selon le cas:

a) pour les fournisseurs de services intermédiaires, le nombre d'injonctions reçues des autorités des États membres, y compris les injonctions émises conformément aux articles 9 et 10, classées par type de contenu illicite concerné, l'État membre qui a émis l'injonction et le délai médian nécessaire pour informer de sa réception l'autorité qui a émis l'injonction, ou toute autre autorité spécifiée dans l'injonction, et pour donner suite à l'injonction;

b) pour les fournisseurs de services d'hébergement, le nombre de notifications soumises conformément à l'article 16, classées par type de contenu présumé illicite concerné, le nombre de notifications soumises par les signaleurs de confiance, toute action

entreprise au titre des notifications en précisant si l'action a été entreprise sur la base de la législation ou des conditions générales du fournisseur, le nombre de notifications traitées de manière automatisée et le délai médian nécessaire pour entreprendre l'action;

c) pour les fournisseurs de services intermédiaires, des informations utiles et compréhensibles sur les activités de modération des contenus auxquelles se sont livrés les fournisseurs de leur propre initiative, y compris l'utilisation d'outils automatisés, les mesures prises pour dispenser une formation et une assistance aux personnes chargées de la modération des contenus, le nombre et le type de mesures prises qui affectent la disponibilité, la visibilité et l'accessibilité des informations fournies par les destinataires du service et sur la capacité des destinataires à fournir des informations par l'intermédiaire du service, ainsi que d'autres restrictions connexes du service; les informations communiquées sont classées par type de contenu illicite ou d'infraction aux conditions générales du fournisseur de services, par méthode de détection et par type de restrictions appliquées;

d) pour les fournisseurs de services intermédiaires, le nombre de réclamations reçues par l'intermédiaire des systèmes internes de traitement des réclamations conformément aux conditions générales du fournisseur et, en outre, pour les fournisseurs de plateformes en ligne, conformément à l'article 20, le fondement de ces réclamations, les décisions prises concernant ces réclamations, le délai médian nécessaire pour prendre ces décisions et le nombre de cas dans lesquels ces décisions ont été infirmées;

e) tout recours à des moyens automatisés à des fins de modération des contenus, y compris une description qualitative, une indication des objectifs précis, des indicateurs de la précision et du taux d'erreur possible des moyens automatisés utilisés pour atteindre ces objectifs, et les éventuelles mesures de sauvegarde appliquées.

2. Le paragraphe 1 du présent article ne s'applique pas aux fournisseurs de services intermédiaires qui peuvent être qualifiés de microentreprises ou de petites entreprises telles qu'elles sont définies dans la recommandation 2003/361/CE et qui ne sont pas de très grandes plateformes en ligne au sens de l'article 33 du présent règlement.

3. La Commission peut adopter des actes d'exécution pour établir des modèles concernant la forme, le contenu et d'autres détails des rapports au titre du paragraphe 1 du présent article, y compris des périodes harmonisées pour l'établissement des rapports. Ces actes d'exécution sont adoptés en conformité avec la procédure consultative visée à l'article 88.

SECTION 2

Dispositions supplémentaires applicables aux fournisseurs de services d'hébergement, y compris les plateformes en ligne

Article 16- Mécanismes de notification et d'action

1. Les fournisseurs de services d'hébergement mettent en place des mécanismes permettant à tout particulier ou à toute entité de leur signaler la présence au sein de leur service d'éléments d'information spécifiques que le particulier ou l'entité considère comme du contenu illicite.

Ces mécanismes sont faciles d'accès et d'utilisation et permettent la soumission de notifications exclusivement par voie électronique.

2. Les mécanismes prévus au paragraphe 1 sont de nature à faciliter la soumission de notifications suffisamment précises et dûment étayées. À cette fin, les fournisseurs de services d'hébergement prennent les mesures nécessaires pour permettre et faciliter la soumission de notifications contenant l'ensemble des éléments suivants:

a) une explication suffisamment étayée des raisons pour lesquelles le particulier ou l'entité allègue que les informations en question sont du contenu illicite;

b) une indication claire de l'emplacement électronique exact de ces informations, comme l'URL ou les URL exact(s), et, le cas échéant, des informations complémentaires permettant d'identifier le contenu illicite en fonction du type de contenu et du type spécifique de service d'hébergement;

c) le nom et l'adresse de courrier électronique du particulier ou de l'entité soumettant la notification, sauf dans le cas d'informations considérées comme impliquant une des infractions visées aux articles 3 à 7 de la directive 2011/93/UE;

d) une déclaration confirmant que le particulier ou l'entité soumettant la notification pense, de bonne foi, que les informations et les allégations qu'elle contient sont exactes et complètes.

3. Les notifications visées au présent article sont réputées donner lieu à la connaissance ou à la prise de conscience effective aux fins de l'article 6 de l'élément d'information spécifique concerné lorsqu'elles permettent à un fournisseur diligent de services d'hébergement d'identifier l'illégalité de l'activité ou de l'information concernée sans examen juridique détaillé.

4. Lorsque la notification contient les coordonnées électroniques du particulier ou de l'entité qui l'a soumise, le fournisseur de services d'hébergement envoie, dans les meilleurs délais, un accusé de réception de la notification à ce particulier ou cette entité.

5. Le fournisseur notifie également, dans les meilleurs délais, à ce particulier ou cette entité sa décision concernant les informations auxquelles la notification se rapporte, tout en fournissant des informations sur les possibilités de recours à l'égard de cette décision.

6. Les fournisseurs de services d'hébergement traitent les notifications qu'ils reçoivent au titre des mécanismes prévus au paragraphe 1 et prennent leurs décisions concernant les informations auxquelles les notifications se rapportent en temps opportun, de manière diligente, non arbitraire et objective. Lorsqu'ils font appel à des moyens automatisés aux fins de ce traitement ou de cette prise de décisions, ils incluent des informations sur cette utilisation dans la notification visée au paragraphe 5.

Article 17 - Exposé des motifs

1. Les fournisseurs de services d'hébergement fournissent à tous les destinataires du service affectés un exposé des motifs clair et spécifique pour l'une ou l'autre des restrictions

suivantes imposées au motif que les informations fournies par le destinataire du service constituent un contenu illicite ou sont incompatibles avec leurs conditions générales:

a) toute restriction de la visibilité d'éléments d'information spécifiques fournis par le destinataire du service, y compris le retrait de contenus, le fait de rendre l'accès à des contenus impossible ou le déclassement de contenus;

b) la suspension, la fin ou autre restriction des paiements monétaires;

c) la suspension ou la fin, en tout ou en partie, de la fourniture du service;

d) la suspension ou la suppression du compte du destinataire du service.

2. Le paragraphe 1 s'applique uniquement lorsque les coordonnées électroniques pertinentes sont connues du fournisseur. Il s'applique au plus tard à compter de la date à laquelle la restriction est imposée, indépendamment de la raison pour laquelle ou de la manière dont elle a été imposée.

Le paragraphe 1 ne s'applique pas lorsque les informations constituent un contenu commercial trompeur et de grande diffusion.

3. L'exposé des motifs visé au paragraphe 1 comprend au minimum les informations suivantes:

a) des informations indiquant si la décision implique soit de retirer des informations, de rendre l'accès à celles-ci impossible, de les déclasser, ou de restreindre leur visibilité, soit de suspendre ou de mettre fin aux paiements monétaires liés à ces informations, ou impose d'autres mesures visées au paragraphe 1 en ce qui concerne lesdites informations, et, le cas échéant, le champ d'application territorial de la décision et sa durée;

b) les faits et circonstances sur base desquels la décision a été prise, y compris, le cas échéant, des informations indiquant si la décision a été prise en vertu d'une notification soumise conformément à l'article 16 ou sur la base d'enquêtes d'initiative volontaires et, lorsque cela est strictement nécessaire, l'identité de la personne à l'origine de la notification;

c) le cas échéant, des informations relatives à l'utilisation de moyens automatisés pour prendre la décision, y compris des informations indiquant si la décision a été prise à l'égard de contenus détectés ou identifiés par des moyens automatisés;

d) lorsque la décision concerne des contenus présumés illicites, une référence au fondement juridique sous-jacent et des explications quant aux raisons pour lesquelles ces informations sont considérées comme des contenus illicites sur ce fondement;

e) lorsque la décision se fonde sur l'incompatibilité alléguée des informations avec les conditions générales du fournisseur de services d'hébergement, une référence aux clauses contractuelles sous-jacentes et des explications quant aux raisons pour lesquelles ces informations sont considérées comme incompatibles avec ces clauses;

f) des informations claires et aisément compréhensibles relatives aux possibilités de recours à la disposition du destinataire du service en ce qui concerne cette décision, notamment, le cas échéant, par l'intermédiaire de mécanismes internes de traitement des réclamations, d'un règlement extrajudiciaire des litiges et d'un recours juridictionnel.

4. Les informations fournies par les fournisseurs de services d'hébergement conformément au présent article sont claires et faciles à comprendre et aussi précises et détaillées que cela est raisonnablement possible compte tenu des circonstances données. En particulier, les informations sont de nature à permettre raisonnablement au destinataire du service concerné d'exercer les possibilités de recours visées au paragraphe 3, point f), de manière effective.

5. Le présent article ne s'applique pas aux injonctions visées à l'article 9.

Article 18 -Notification des soupçons d'infraction pénale

1. Lorsqu'un fournisseur de services d'hébergement a connaissance d'informations conduisant à soupçonner qu'une infraction pénale présentant une menace pour la vie ou la sécurité d'une ou de plusieurs personnes a été commise, est en train d'être commise ou est susceptible d'être commise, il informe promptement les autorités répressives ou judiciaires de l'État membre ou des États membres concernés de son soupçon et fournit toutes les informations pertinentes disponibles.

2. Lorsque le fournisseur de services d'hébergement n'est pas en mesure de déterminer avec une certitude raisonnable l'État membre concerné, il informe les autorités répressives de l'État membre dans lequel il est établi ou dans lequel son représentant légal réside ou est établi ou informe Europol, ou les deux.

Aux fins du présent article, l'État membre concerné est l'État membre dans lequel l'infraction est suspectée d'avoir été commise, d'être commise ou est susceptible d'être commise, ou l'État membre dans lequel l'auteur présumé de l'infraction réside ou se trouve, ou l'État membre dans lequel la victime de l'infraction suspectée réside ou se trouve.

SECTION 3

Dispositions supplémentaires applicables aux fournisseurs de plateformes en ligne

Article 19- Exclusion des microentreprises et petites entreprises

1. La présente section, à l'exception de son article 24, paragraphe 3, ne s'applique pas aux fournisseurs de plateformes en ligne qui peuvent être qualifiés de microentreprises ou de petites entreprises telles qu'elles sont définies dans la recommandation 2003/361/CE.

La présente section, à l'exception de son article 24, paragraphe 3, ne s'applique pas aux fournisseurs de plateformes en ligne qui étaient qualifiés précédemment de microentreprises ou de petites entreprises telles qu'elles sont définies dans la recommandation 2003/361/CE, pendant les douze mois qui suivent la perte de ce statut en vertu de l'article 4, paragraphe 2, de ladite recommandation, sauf lorsqu'il s'agit de très grandes plateformes en ligne conformément à l'article 33.

2. Par dérogation au paragraphe 1 du présent article, la présente section s'applique aux fournisseurs de plateformes en ligne qui ont été désignés comme des très grandes plateformes en ligne conformément à l'article 33, indépendamment du fait qu'ils soient qualifiés de microentreprises ou de petites entreprises.

Article 20- Système interne de traitement des réclamations

1. Les fournisseurs de plateformes en ligne fournissent aux destinataires du service, y compris aux particuliers ou aux entités qui ont soumis une notification, pour une période d'au moins six mois suivant la décision visée dans le présent paragraphe, l'accès à un système interne de traitement des réclamations efficace qui leur permet d'introduire, par voie électronique et gratuitement, des réclamations contre la décision prise par le fournisseur de la plateforme en ligne à la suite de la réception d'une notification ou contre les décisions suivantes prises par le fournisseur de la plateforme en ligne au motif que les informations fournies par les destinataires constituent un contenu illicite ou qu'elles sont incompatibles avec ses conditions générales:

a) les décisions sur la question de savoir s'il y a lieu ou non de retirer les informations, de rendre l'accès à celles-ci impossible ou de restreindre leur visibilité;

b) les décisions sur la question de savoir s'il y a lieu ou non de suspendre ou de mettre fin, en tout ou en partie, à la fourniture du service aux destinataires;

c) les décisions sur la question de savoir s'il y a lieu ou non de suspendre ou de supprimer le compte des destinataires;

d) les décisions sur la question de savoir s'il y a lieu ou non de suspendre la capacité de monétiser les informations fournies par les destinataires, de mettre fin à cette capacité ou de restreindre d'une autre manière cette capacité.

2. La période d'au moins six mois visée au paragraphe 1 du présent article court à partir du jour où le destinataire du service est informé de la décision, conformément à l'article 16, paragraphe 5, ou à l'article 17.

3. Les fournisseurs de plateformes en ligne veillent à ce que leurs systèmes internes de traitement des réclamations soient d'un accès et d'une utilisation aisés et permettent et facilitent la soumission de réclamations suffisamment précises et dûment étayées.

4. Les fournisseurs de plateformes en ligne traitent les réclamations soumises par l'intermédiaire de leurs systèmes internes de traitement des réclamations en temps opportun, de manière non discriminatoire, diligente et non arbitraire. Lorsqu'une réclamation contient suffisamment de motifs pour que le fournisseur de la plateforme en ligne considère que sa décision de ne pas agir à la suite de la notification est infondée ou que les informations auxquelles la réclamation se rapporte ne sont pas illicites et ne sont pas incompatibles avec ses conditions générales, ou lorsqu'elle contient des informations indiquant que la conduite du plaignant ne justifie pas la mesure prise, le fournisseur infirme sa décision visée au paragraphe 1 dans les meilleurs délais.

5. Les fournisseurs de plateformes en ligne informent les plaignants dans les meilleurs délais de la décision motivée qu'ils prennent en ce qui concerne les informations auxquelles la

réclamation se rapporte et de la possibilité d'avoir accès à un règlement extrajudiciaire des litiges prévue à l'article 21 et des autres possibilités de recours disponibles.

6. Les fournisseurs de plateformes en ligne veillent à ce que les décisions visées au paragraphe 5 soient prises sous le contrôle de collaborateurs dûment qualifiés, et pas uniquement par des moyens automatisés.

Article 21- Règlement extrajudiciaire des litiges

1. Les destinataires du service, y compris les particuliers ou les entités qui ont soumis des notifications, qui sont destinataires des décisions visées à l'article 20, paragraphe 1, ont le droit de choisir tout organe de règlement extrajudiciaire des litiges qui a été certifié conformément au paragraphe 3 du présent article en vue de résoudre les litiges relatifs à ces décisions, y compris pour les réclamations qui n'ont pas été résolues par le système interne de traitement des réclamations visé audit article.

Les fournisseurs de plateformes en ligne veillent à ce que les informations relatives à la possibilité pour les destinataires du service d'avoir accès à un règlement extrajudiciaire des litiges, conformément au premier alinéa, soient facilement accessibles sur leur interface en ligne, claires et aisément compréhensibles.

Le premier alinéa est sans préjudice du droit du destinataire du service concerné d'engager, à tout moment, une procédure pour contester lesdites décisions prises par les fournisseurs de plateformes en ligne devant une juridiction conformément au droit applicable.

2. Les deux parties s'engagent, de bonne foi, avec l'organe de règlement extrajudiciaire des litiges certifié qui est choisi en vue de résoudre le litige.

Les fournisseurs de plateformes en ligne peuvent refuser de s'engager avec cet organe de règlement extrajudiciaire des litiges si un litige concernant les mêmes informations et les mêmes motifs d'illégalité ou d'incompatibilité alléguée du contenu a déjà été résolu.

L'organe de règlement extrajudiciaire des litiges certifié n'a pas le pouvoir d'imposer aux parties un règlement du litige contraignant.

3. Le coordinateur pour les services numériques de l'État membre dans lequel est établi l'organe de règlement extrajudiciaire des litiges certifie cet organe, à sa demande, pour une période maximale de cinq ans, qui peut être renouvelée, lorsque l'organe a démontré qu'il remplit l'ensemble des conditions suivantes:

a) il est impartial et indépendant, y compris financièrement indépendant, des fournisseurs de plateformes en ligne et des destinataires du service fourni par les fournisseurs de plateformes en ligne, y compris des particuliers ou des entités qui ont soumis des notifications;

b) il dispose de l'expertise nécessaire en ce qui concerne les questions liées à un ou plusieurs domaines particuliers de contenu illicite, ou en ce qui concerne l'application et la mise en application des conditions générales d'un ou de plusieurs types de plateformes en ligne, lui permettant de contribuer efficacement au règlement d'un litige;

c) ses membres ne sont pas rémunérés en fonction de l'issue de la procédure;

d) processus de règlement extrajudiciaire des litiges qu'il propose est facilement accessible au moyen d'une technologie des communications électroniques et prévoit la possibilité d'engager le processus de règlement des litiges et de soumettre les documents justificatifs nécessaires en ligne;

e) il est en mesure de régler des litiges de manière rapide, efficace et économiquement avantageuse, et dans au minimum une des langues officielles des institutions de l'Union;

f) le processus de règlement extrajudiciaire des litiges qu'il propose se déroule conformément à des règles de procédure claires et équitables, qui sont aisément et publiquement accessibles et qui respectent le droit applicable, y compris le présent article.

Le cas échéant, le coordinateur pour les services numériques précise dans le certificat:

a) les questions particulières sur lesquelles porte l'expertise de l'organe, visées au premier alinéa, point b); et

b) la ou les langues officielles des institutions de l'Union dans laquelle ou lesquelles l'organe est en mesure de régler des litiges, comme il est prévu au premier alinéa, point e).

4. Les organes de règlement extrajudiciaire des litiges certifiés font rapport, une fois par an, au coordinateur pour les services numériques qui les a certifiés, sur leur fonctionnement, en précisant au moins le nombre de litiges qu'ils ont reçus, les informations sur l'issue de ces litiges, le laps de temps moyen nécessaire à leur résolution et les éventuelles lacunes ou difficultés rencontrées. Ils fournissent des informations supplémentaires à la demande dudit coordinateur pour les services numériques.

Les coordinateurs pour les services numériques établissent tous les deux ans un rapport sur le fonctionnement des organes de règlement extrajudiciaire des litiges qu'ils ont certifiés. En particulier, ce rapport:

a) Indique le nombre de litiges que chaque organe de règlement extrajudiciaire des litiges certifié a reçus chaque année;

b) Indique l'issue des procédures portées devant ces organes et le laps de temps moyen nécessaire à la résolution des litiges;

c) Recense et explique les éventuelles lacunes ou difficultés systématiques ou sectorielles rencontrées en rapport avec le fonctionnement de ces organes;

d) Recense les bonnes pratiques concernant ce fonctionnement;

e) Formule, le cas échéant, des recommandations sur la manière d'améliorer ce fonctionnement.

Les organes de règlement extrajudiciaire des litiges certifiés mettent leurs décisions à la disposition des parties dans un délai raisonnable et au plus tard 90 jours civils après la réception de la plainte. En cas de litiges très complexes, l'organe de règlement extrajudiciaire des litiges certifié peut, de sa propre initiative, prolonger le délai de 90 jours civils, pour une période supplémentaire n'excédant pas 90 jours, dans la limite d'une durée totale maximale de 180 jours.

5. Lorsque l'organe de règlement extrajudiciaire des litiges se prononce sur le litige en faveur du destinataire du service, y compris le particulier ou l'entité qui a soumis une notification, le fournisseur de la plateforme en ligne supporte tous les frais facturés par l'organe de règlement extrajudiciaire des litiges et rembourse à ce destinataire, y compris le particulier ou l'entité, toute autre dépense raisonnable qu'il a effectuée en lien avec le règlement du litige. Lorsque l'organe de règlement extrajudiciaire des litiges se prononce sur le litige en faveur du fournisseur de la plateforme en ligne, le destinataire du service, y compris le particulier ou l'entité, n'est pas tenu de rembourser les frais ou autres dépenses que le fournisseur de la plateforme en ligne a engagés ou dont il est redevable en lien avec le règlement du litige, à moins que l'organe de règlement extrajudiciaire des litiges constate que ce destinataire a manifestement agi de mauvaise foi.

Les frais facturés par l'organe de règlement extrajudiciaire des litiges aux fournisseurs de plateformes en ligne pour le règlement du litige sont raisonnables et n'excèdent en aucun cas les coûts engagés par l'organe. Pour les destinataires du service, le règlement du litige est accessible gratuitement ou moyennant une somme symbolique.

Les organes de règlement extrajudiciaire des litiges certifiés informent le destinataire du service, y compris les particuliers ou les entités qui ont soumis une notification, et le fournisseur de la plateforme en ligne concerné, des frais ou des mécanismes employés pour calculer les frais, avant le début du processus de règlement du litige.

6. Les États membres peuvent établir des organes de règlement extrajudiciaire des litiges aux fins du paragraphe 1 ou apporter un soutien aux activités de certains ou de tous les organes de règlement extrajudiciaire des litiges qu'ils ont certifiés conformément au paragraphe 3.

Les États membres veillent à ce qu'aucune des activités qu'ils entreprennent au titre du premier alinéa ne nuise à la capacité de leurs coordinateurs pour les services numériques à certifier les organes concernés conformément au paragraphe 3.

7. Le coordinateur pour les services numériques qui a certifié un organe de règlement extrajudiciaire des litiges révoque cette certification s'il constate, à la suite d'une enquête menée soit de sa propre initiative, soit sur la base d'informations reçues de tiers, que l'organe de règlement extrajudiciaire des litiges ne remplit plus les conditions énoncées au paragraphe 3. Avant de révoquer cette certification, le coordinateur pour les services numériques donne à cet organe la possibilité de réagir aux conclusions de son enquête et à son intention de révoquer la certification de l'organe de règlement extrajudiciaire des litiges.

8. Les coordinateurs pour les services numériques notifient à la Commission la liste des organes de règlement extrajudiciaire des litiges qu'ils ont certifiés conformément au paragraphe 3, y compris, le cas échéant, les spécifications visées au second alinéa dudit paragraphe, ainsi que la liste des organes de règlement extrajudiciaire des litiges dont ils ont

révoqué la certification. La Commission publie et tient à jour une liste de ces organes, comprenant ces spécifications, sur un site internet dédié, facilement accessible, prévu à cet effet.

9. Le présent article est sans préjudice de la directive 2013/11/UE et des procédures et entités de règlement extrajudiciaire des litiges de consommation qu'elle établit.

Article 22- Signaleurs de confiance

1. Les fournisseurs de plateformes en ligne prennent les mesures techniques et organisationnelles nécessaires pour veiller à ce que les notifications soumises par des signaleurs de confiance, agissant dans leur domaine d'expertise désigné, par l'intermédiaire des mécanismes visés à l'article 16, soient prioritaires et soient traitées et donnent lieu à des décisions dans les meilleurs délais.

2. Le statut de signaleur de confiance au titre du présent règlement est attribué, sur demande présentée par une entité, quelle qu'elle soit, par le coordinateur pour les services numériques de l'État membre dans lequel l'entité présentant la demande est établie, à l'entité présentant la demande qui a démontré qu'elle remplit l'ensemble des conditions suivantes:

a) elle dispose d'une expertise et de compétences particulières aux fins de détecter, d'identifier et de notifier des contenus illicites;

b) elle est indépendante de tout fournisseur de plateformes en ligne;

c) elle exerce ses activités aux fins de la soumission des notifications de manière diligente, précise et objective.

3. Les signaleurs de confiance publient, au minimum une fois par an, des rapports détaillés et facilement compréhensibles sur les notifications soumises conformément à l'article 16 pendant la période concernée. Le rapport indique au moins le nombre de notifications, classées selon les critères suivants:

a) L'identité du fournisseur de services d'hébergement;

b) Le type de contenu présumé illicite notifié;

c) l'action entreprise par le fournisseur.

Ces rapports comprennent une explication des procédures mises en place pour garantir que le signaleur de confiance conserve son indépendance.

Les signaleurs de confiance envoient ces rapports au coordinateur pour les services numériques qui a attribué le statut de signaleur de confiance et les mettent à la disposition du public. Les informations figurant dans ces rapports ne contiennent pas de données à caractère personnel.

4. Les coordinateurs pour les services numériques communiquent à la Commission et au comité les noms, adresses postales et adresses de courrier électronique des entités auxquelles ils ont attribué le statut de signaleur de confiance conformément au paragraphe 2 ou dont ils

ont suspendu le statut de signaleur de confiance conformément au paragraphe 6 ou révoqué ledit statut conformément au paragraphe 7.

5. La Commission publie les informations visées au paragraphe 4 dans une base de données mise à la disposition du public, dans un format facilement accessible et lisible par une machine, et tient à jour cette base de données.

6. Lorsqu'un fournisseur de plateformes en ligne dispose d'informations indiquant qu'un signaleur de confiance a soumis, par l'intermédiaire des mécanismes visés à l'article 16, un nombre significatif de notifications manquant de précision, inexactes ou insuffisamment étayées, notamment des informations recueillies en lien avec le traitement de réclamations par des systèmes internes de traitement des réclamations visés à l'article 20, paragraphe 4, il communique ces informations au coordinateur pour les services numériques qui a attribué le statut de signaleur de confiance à l'entité concernée, en fournissant les explications et les documents justificatifs nécessaires. Dès réception des informations fournies par le fournisseur de plateformes en ligne et si le coordinateur pour les services numériques estime qu'il existe des raisons légitimes d'ouvrir une enquête, le statut de signaleur de confiance est suspendu pendant la durée de l'enquête. Cette enquête est menée dans les meilleurs délais.

7. Le coordinateur pour les services numériques qui a attribué le statut de signaleur de confiance à une entité révoque ce statut s'il constate, à la suite d'une enquête menée soit de sa propre initiative, soit sur la base d'informations reçues de tiers, y compris les informations fournies par un fournisseur de plateformes en ligne en vertu du paragraphe 6, que l'entité ne remplit plus les conditions énoncées au paragraphe 2. Avant de révoquer ce statut, le coordinateur pour les services numériques donne à l'entité la possibilité de réagir aux conclusions de son enquête et à son intention de révoquer le statut de signaleur de confiance de l'entité.

8. La Commission, après avoir consulté le comité, publie, si nécessaire, des lignes directrices pour aider les fournisseurs de plateformes en ligne et les coordinateurs pour les services numériques à appliquer les paragraphes 2, 6 et 7.

Article 23- Mesures de lutte et de protection contre les utilisations abusives

1. Les fournisseurs de plateformes en ligne suspendent, pendant une période raisonnable et après avoir émis un avertissement préalable, la fourniture de leurs services aux destinataires du service qui fournissent fréquemment des contenus manifestement illicites.

2. Les fournisseurs de plateformes en ligne suspendent, pendant une période raisonnable et après avoir émis un avertissement préalable, le traitement des notifications et des réclamations soumises par l'intermédiaire des mécanismes de notification et d'action et des systèmes internes de traitement des réclamations prévus aux articles 16 et 20, respectivement, par des particuliers, des entités ou des plaignants qui soumettent fréquemment des notifications ou des réclamations manifestement infondées.

3. Lorsqu'ils décident d'une suspension, les fournisseurs de plateformes en ligne apprécient au cas par cas et en temps opportun, de manière diligente et objective, si le destinataire du service, le particulier, l'entité ou le plaignant se livre aux utilisations abusives visées aux paragraphes 1 et 2, en tenant compte de l'ensemble des faits et circonstances pertinents qui

ressortent des informations dont ils disposent. Ces circonstances comprennent au moins les éléments suivants:

a) le nombre, en valeur absolue, d'éléments de contenus manifestement illicites ou de notifications ou de réclamations manifestement infondées, soumis au cours d'une période donnée;

b) la proportion relative de ces éléments par rapport au nombre total d'éléments d'information fournis ou de notifications soumises au cours d'une période donnée;

c) la gravité des utilisations abusives, y compris la nature des contenus illicites, et de leurs conséquences;

d) Lorsqu'il est possible de la déterminer, l'intention du destinataire du service, du particulier, de l'entité ou du plaignant.

4. Les fournisseurs de plateformes en ligne énoncent de manière claire et détaillée, dans leurs conditions générales, leur politique relative aux utilisations abusives visées aux paragraphes 1 et 2, et donnent des exemples des faits et circonstances dont ils tiennent compte pour apprécier si certains comportements constituent des utilisations abusives et déterminer la durée de la suspension.

Article 24 - Obligations en matière de rapports de transparence incombant aux fournisseurs de plateformes en ligne

1. En plus des informations visées à l'article 15, les fournisseurs de plateformes en ligne intègrent aux rapports visés dans cet article des informations sur les points suivants:

a) le nombre de litiges transmis aux organes de règlement extrajudiciaire des litiges visés à l'article 21, les résultats du règlement des litiges, le délai médian nécessaire pour mener à bien les procédures de règlement des litiges et la proportion de litiges pour lesquels le fournisseur de la plateforme en ligne a mis en œuvre les décisions de l'organe;

b) le nombre de suspensions imposées au titre de l'article 23, en faisant la distinction entre les suspensions prononcées en raison de la fourniture de contenus manifestement illicites, de la soumission de notifications manifestement infondées et de la soumission de réclamations manifestement infondées.

2. Au plus tard le 17 février 2023 et au moins tous les six mois par la suite, les fournisseurs publient pour chaque plateforme en ligne ou chaque moteur de recherche en ligne, dans une section de leur interface en ligne accessible au public, des informations relatives à la moyenne mensuelle des destinataires actifs du service dans l'Union, calculée sous forme de moyenne au cours des six derniers mois et conformément à la méthodologie établie dans les actes délégués visés à l'article 33, paragraphe 3, lorsque ces actes délégués ont été adoptés.

3. Les fournisseurs de plateformes en ligne ou de moteurs de recherche en ligne communiquent au coordinateur pour les services numériques de l'État membre d'établissement et à la Commission, à leur demande et dans les meilleurs délais, les informations visées au paragraphe 2, mises à jour jusqu'au moment de la demande. Ledit

coordinateur pour les services numériques ou la Commission peuvent demander au fournisseur de la plateforme en ligne ou du moteur de recherche en ligne de fournir des informations complémentaires concernant le calcul visé audit paragraphe, y compris des explications et des justifications quant aux données utilisées. Ces informations ne contiennent pas de données à caractère personnel.

4. Lorsque le coordinateur pour les services numériques de l'État membre d'établissement a des raisons de considérer, sur la base des informations reçues en application des paragraphes 2 et 3 du présent article, qu'un fournisseur de plateformes en ligne ou de moteurs de recherche en ligne atteint le seuil du nombre mensuel moyen de destinataires actifs du service dans l'Union fixé à l'article 33, paragraphe 1, il en informe la Commission.

5. Les fournisseurs de plateformes en ligne soumettent à la Commission, dans les meilleurs délais, les décisions et les exposés des motifs visés à l'article 17, paragraphe 1, en vue de leur inclusion dans une base de données accessible au public, lisible par une machine, et gérée par la Commission. Les fournisseurs de plateformes en ligne veillent à ce que les informations soumises ne contiennent pas de données à caractère personnel.

6. La Commission peut adopter des actes d'exécution pour établir des modèles concernant la forme, le contenu et d'autres détails des rapports au titre du paragraphe 1 du présent article. Ces actes d'exécution sont adoptés en conformité avec la procédure consultative visée à l'article 88.

Article 25 - Conception et organisation des interfaces en ligne

1. Les fournisseurs de plateformes en ligne ne conçoivent, n'organisent ni n'exploitent leurs interfaces en ligne de façon à tromper ou à manipuler les destinataires de leur service ou de toute autre façon propre à altérer ou à entraver substantiellement la capacité des destinataires de leur service à prendre des décisions libres et éclairées.

2. L'interdiction contenue dans le paragraphe 1 ne s'applique pas aux pratiques couvertes par la directive 2005/29/CE ou le règlement (UE) 2016/679.

3. La Commission peut publier des lignes directrices sur la manière dont le paragraphe 1 s'applique à des pratiques spécifiques, notamment:

a) Accorder davantage d'importance à certains choix au moment de demander au destinataire du service de prendre une décision;

b) Demander de façon répétée au destinataire du service de faire un choix lorsque ce choix a déjà été fait, notamment en faisant apparaître une fenêtre contextuelle qui perturbe l'expérience de l'utilisateur;

c) Rendre la procédure de désinscription d'un service plus compliquée que l'inscription à celui-ci.

Article 26 - Publicité sur les plateformes en ligne

1. Les fournisseurs de plateformes en ligne qui présentent de la publicité sur leurs interfaces en ligne veillent à ce que, pour chaque publicité spécifique présentée à chaque destinataire

individuel, les destinataires du service puissent de manière claire, précise, non ambiguë et en temps réel:

a) Se rendre compte que les informations sont de la publicité, y compris au moyen de marquages bien visibles qui pourraient suivre des normes en vertu de l'article 44;

b) Identifier la personne physique ou morale pour le compte de laquelle la publicité est présentée;

c) Identifier la personne physique ou morale qui a payé pour la publicité, si cette personne est différente de la personne physique ou morale visée au point b); et

d) Déterminer les informations utiles, qui doivent être directement et facilement accessibles à partir de la publicité, concernant les principaux paramètres utilisés pour déterminer le destinataire auquel la publicité est présentée et, le cas échéant, la manière dont ces paramètres peuvent être modifiés.

2. Les fournisseurs de plateformes en ligne fournissent aux destinataires du service une fonctionnalité leur permettant de déclarer si le contenu qu'ils fournissent constitue une communication commerciale ou s'il contient une telle communication.

Lorsque le destinataire du service soumet une déclaration en vertu du présent paragraphe, le fournisseur de plateformes en ligne veille à ce que les autres destinataires du service puissent se rendre compte de manière claire, non ambiguë et en temps réel, y compris au moyen de marquages bien visibles, qui pourraient suivre des normes en vertu de l'article 44, que le contenu fourni par le destinataire du service constitue une communication commerciale ou contient une telle communication, telle qu'elle est décrite dans cette déclaration.

3. Les fournisseurs de plateformes en ligne ne présentent pas aux destinataires du service de publicité qui repose sur du profilage, tel qu'il est défini à l'article 4, point 4), du règlement (UE) 2016/679, en utilisant les catégories particulières de données à caractère personnel visées à l'article 9, paragraphe 1, du règlement (UE) 2016/679.

Article 27 - Transparence du système de recommandation

1. Les fournisseurs de plateformes en ligne qui utilisent des systèmes de recommandation établissent dans leurs conditions générales, dans un langage simple et compréhensible, les principaux paramètres utilisés dans leurs systèmes de recommandation, ainsi que les options dont disposent les destinataires du service pour modifier ou influencer ces principaux paramètres.

2. Les principaux paramètres visés au paragraphe 1 expliquent pourquoi certaines informations sont suggérées au destinataire du service. Ils précisent, au minimum:

a) les critères les plus importants pour déterminer les informations suggérées au destinataire du service;

b) les raisons de l'importance relative de ces paramètres.

3. Lorsque plusieurs options sont disponibles conformément au paragraphe 1 pour les systèmes de recommandation qui déterminent l'ordre relatif des informations présentées aux destinataires du service, les fournisseurs de plateformes en ligne prévoient également une fonctionnalité permettant aux destinataires du service de sélectionner et de modifier à tout moment leur option favorite. Cette fonctionnalité est directement et aisément accessible dans la rubrique spécifique de l'interface de la plateforme en ligne où les informations sont hiérarchisées.

Article 28 -Protection des mineurs en ligne

1. Les fournisseurs de plateformes en ligne accessibles aux mineurs mettent en place des mesures appropriées et proportionnées pour garantir un niveau élevé de protection de la vie privée, de sûreté et de sécurité des mineurs sur leur service.

2. Les fournisseurs de plateformes en ligne ne présentent pas sur leur interface de publicité qui repose sur du profilage, tel qu'il est défini à l'article 4, point 4), du règlement (UE) 2016/679 en utilisant des données à caractère personnel concernant le destinataire du service dès lors qu'ils ont connaissance avec une certitude raisonnable que le destinataire du service est un mineur.

3. Le respect des obligations énoncées dans le présent article n'impose pas aux fournisseurs de plateformes en ligne de traiter des données à caractère personnel supplémentaires afin de déterminer si le destinataire du service est un mineur.

4. La Commission, après avoir consulté le comité, peut publier des lignes directrices pour aider les fournisseurs de plateformes en ligne à appliquer le paragraphe 1.

SECTION 4

Dispositions supplémentaires applicables aux fournisseurs de plateformes en ligne permettant aux consommateurs de conclure des contrats à distance avec des professionnels

Article 29 - Exclusion des microentreprises et petites entreprises

1. La présente section ne s'applique pas aux fournisseurs de plateformes en ligne permettant aux consommateurs de conclure des contrats à distance avec des professionnels qui peuvent être qualifiés de microentreprises ou de petites entreprises telles qu'elles sont définies dans la recommandation 2003/361/CE.

La présente section ne s'applique pas aux fournisseurs de plateformes en ligne permettant aux consommateurs de conclure des contrats à distance avec des professionnels qui étaient qualifiés précédemment de microentreprises ou de petites entreprises telles qu'elles sont définies dans la recommandation 2003/361/CE, pendant les douze mois qui suivent la perte de ce statut en vertu de l'article 4, paragraphe 2, de ladite recommandation, sauf s'il s'agit de très grandes plateformes en ligne conformément à l'article 33.

2. Par dérogation au paragraphe 1 du présent article, la présente section s'applique aux fournisseurs de plateformes en ligne permettant aux consommateurs de conclure des contrats

à distance avec des professionnels qui ont été désignés comme des très grandes plateformes en ligne conformément à l'article 33, indépendamment du fait qu'ils soient qualifiés de microentreprises ou de petites entreprises.

Article 30 - Traçabilité des professionnels

1. Les fournisseurs de plateformes en ligne permettant aux consommateurs de conclure des contrats à distance avec des professionnels veillent à ce que ces derniers puissent uniquement utiliser ces plateformes en ligne pour promouvoir des messages relatifs à des produits ou services ou proposer des produits ou services à des consommateurs situés dans l'Union si, avant l'utilisation de leurs services à ces fins, ils ont obtenu les informations suivantes, lorsque cela s'applique au professionnel:

a) le nom, l'adresse, le numéro de téléphone et l'adresse de courrier électronique du professionnel;

b) un exemplaire du document d'identification du professionnel ou toute autre identification électronique telle qu'elle est définie à l'article 3 du règlement (UE) n° 910/2014 du Parlement européen et du Conseil (40);

c) les coordonnées du compte de paiement du professionnel;

d) lorsque le professionnel est inscrit à un registre commercial ou un registre public similaire, le registre du commerce auquel le professionnel est inscrit et son numéro d'enregistrement ou un moyen équivalent d'identification dans ce registre;

e) une autocertification du professionnel par laquelle il s'engage à ne fournir que des produits ou services conformes aux règles applicables du droit de l'Union.

2. Lorsqu'il reçoit les informations visées au paragraphe 1, et avant d'autoriser le professionnel concerné à utiliser ses services, le fournisseur de la plateforme en ligne permettant aux consommateurs de conclure des contrats à distance avec des professionnels déploie tous ses efforts pour évaluer si les informations visées au paragraphe 1, points a) à e), sont fiables et complètes, au moyen de toute base de données ou interface en ligne officielle, libre d'accès, mise à disposition par un État membre ou l'Union, ou en demandant au professionnel de fournir des documents justificatifs provenant de sources fiables. Aux fins du présent règlement, les professionnels sont responsables de l'exactitude des informations fournies.

Pour ce qui concerne les professionnels qui utilisent déjà les services de fournisseurs de plateformes en ligne permettant aux consommateurs de conclure des contrats à distance avec des professionnels, aux fins visées au paragraphe 1, à la date du 17 février 2024, le fournisseur déploie tous ses efforts pour obtenir du professionnel concerné les informations énumérées dans un délai de douze mois. Lorsque le professionnel concerné ne fournit pas les informations dans ce délai, le fournisseur suspend la fourniture de ses services à ce professionnel jusqu'à ce que celui-ci ait communiqué toutes les informations en question.

3. Lorsque le fournisseur de la plateforme en ligne permettant aux consommateurs de conclure des contrats à distance avec des professionnels dispose de suffisamment d'indices ou a des raisons de penser qu'un élément d'information visé au paragraphe 1 obtenu du

professionnel concerné est inexact, incomplet ou obsolète, ce fournisseur demande au professionnel de remédier à cette situation, dans les meilleurs délais ou dans le délai prévu par le droit de l'Union et le droit national.

Lorsque le professionnel ne corrige pas ou ne complète pas cette information, le fournisseur de la plateforme en ligne permettant aux consommateurs de conclure des contrats à distance avec des professionnels suspend rapidement la fourniture de son service audit professionnel en ce qui concerne l'offre de produits ou de services aux consommateurs situés dans l'Union, jusqu'à ce que la demande soit entièrement satisfaite.

4. Sans préjudice de l'article 4 du règlement (UE) 2019/1150, si le fournisseur d'une plateforme en ligne permettant aux consommateurs de conclure des contrats à distance avec des professionnels refuse d'autoriser un professionnel à utiliser son service en vertu du paragraphe 1 ou suspend la fourniture de son service en vertu du paragraphe 3 du présent article, le professionnel concerné a le droit d'introduire une réclamation conformément aux articles 20 et 21 du présent règlement.

5. Les fournisseurs de plateformes en ligne permettant aux consommateurs de conclure des contrats à distance avec des professionnels stockent les informations obtenues au titre des paragraphes 1 et 2 de façon sécurisée pour une durée de six mois après la fin de leur relation contractuelle avec le professionnel concerné. Ils suppriment par la suite ces informations.

6. Sans préjudice du paragraphe 2 du présent article, le fournisseur de la plateforme en ligne permettant aux consommateurs de conclure des contrats à distance avec des professionnels ne divulgue les informations à des tiers que lorsqu'il y est tenu conformément au droit applicable, y compris les injonctions visées à l'article 10 et toute injonction émise par les autorités compétentes des États membres ou la Commission aux fins de l'exécution des missions qui leur incombent au titre du présent règlement.

7. Le fournisseur de la plateforme en ligne permettant aux consommateurs de conclure des contrats à distance avec des professionnels met les informations énumérées au paragraphe 1, points a), d) et e), à la disposition des destinataires du service, de manière claire, aisément accessible et compréhensible. Ces informations sont disponibles au moins sur l'interface en ligne de la plateforme en ligne où les informations sur le produit ou le service sont présentées.

Article 31 - Conformité dès la conception

1. Les fournisseurs de plateformes en ligne permettant aux consommateurs de conclure des contrats à distance avec des professionnels veillent à ce que leur interface en ligne soit conçue et organisée d'une manière permettant aux professionnels de respecter leurs obligations en matière d'informations précontractuelles, de conformité et d'informations sur la sécurité des produits qui leur incombent en vertu du droit applicable de l'Union.

En particulier, le fournisseur concerné veille à ce que son interface en ligne permette aux professionnels de fournir des informations concernant le nom, l'adresse, le numéro de téléphone et l'adresse de courrier électronique de l'opérateur économique, tel qu'il est défini à l'article 3, point 13), du règlement (UE) 2019/1020 et dans d'autres dispositions du droit de l'Union.

2. Les fournisseurs de plateformes en ligne permettant aux consommateurs de conclure des contrats à distance avec des professionnels conçoivent et organisent leur interface en ligne de manière à permettre aux professionnels de fournir au moins ce qui suit:

a) les informations nécessaires à l'identification claire et sans ambiguïté des produits ou services promus ou proposés aux consommateurs situés dans l'Union par l'intermédiaire des services des fournisseurs;

b) tout signe permettant d'identifier le professionnel, tel que la marque, un symbole ou un logo; et

c) le cas échéant, les informations concernant l'étiquetage et le marquage conformément aux règles du droit de l'Union applicable en matière de sécurité et de conformité des produits.

3. Les fournisseurs de plateformes en ligne permettant aux consommateurs de conclure des contrats à distance avec des professionnels déploient tous leurs efforts pour déterminer si ces professionnels ont communiqué les informations visées aux paragraphes 1 et 2 avant de les autoriser à proposer leurs produits ou leurs services sur lesdites plateformes. Après avoir autorisé le professionnel à proposer des produits ou des services sur sa plateforme en ligne permettant aux consommateurs de conclure des contrats à distance avec des professionnels, le fournisseur s'efforce, dans la mesure du raisonnable, de vérifier de manière aléatoire, dans une base de données en ligne ou une interface en ligne officielle, librement accessible et lisible par une machine, si les produits ou services proposés ont été recensés comme étant illégaux.

Article 32 - Droit à l'information

1. Lorsque le fournisseur d'une plateforme en ligne permettant aux consommateurs de conclure des contrats à distance avec des professionnels a connaissance, par quelque moyen que ce soit, qu'un professionnel propose un produit ou service illégal à des consommateurs situés dans l'Union par l'intermédiaire de ses services, ledit fournisseur informe, dans la mesure où il dispose de leurs coordonnées, les consommateurs qui ont acheté le produit ou le service illégal en question par l'intermédiaire de ses services, de ce qui suit:

a) le fait que le produit ou service est illégal;

b) l'identité du professionnel; et

c) tout moyen de recours pertinent.

L'obligation prévue au premier alinéa est limitée aux achats de produits ou services illégaux réalisés dans les six mois précédant le moment où le fournisseur a eu connaissance de l'illégalité.

2. Lorsque, dans la situation visée au paragraphe 1, le fournisseur de la plateforme en ligne permettant aux consommateurs de conclure des contrats à distance avec des professionnels ne dispose pas des coordonnées de tous les consommateurs concernés, il met à la disposition du public, de manière facilement accessible, sur son interface en ligne des informations

concernant les produits ou services illégaux, l'identité du professionnel et les voies de recours pertinentes.

SECTION 5

Obligations supplémentaires de gestion des risques systémiques imposées aux fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne

Article 33 - Très grandes plateformes en ligne et très grands moteurs de recherche en ligne

1. La présente section s'applique aux plateformes en ligne et aux moteurs de recherche en ligne qui ont un nombre mensuel moyen de destinataires actifs du service dans l'Union égal ou supérieur à 45 millions, et qui sont désignés comme des très grandes plateformes en ligne ou des très grands moteurs de recherche en ligne en vertu du paragraphe 4.

2. La Commission adopte des actes délégués conformément à l'article 87 pour ajuster le nombre mensuel moyen de destinataires actifs du service dans l'Union visé au paragraphe 1 lorsque la population de l'Union augmente ou diminue d'au moins 5 % par rapport à sa population de 2020 ou par rapport à sa population après un ajustement effectué au moyen d'un acte délégué dans l'année au cours de laquelle le dernier acte délégué en date a été adopté. Dans ce cas de figure, elle ajuste le nombre de manière à ce qu'il corresponde à 10 % de la population de l'Union dans l'année au cours de laquelle elle adopte l'acte délégué, arrondi à la hausse ou à la baisse de sorte que le nombre puisse être exprimé en millions.

3. La Commission peut adopter des actes délégués, conformément à l'article 87, après avoir consulté le comité, pour compléter les dispositions du présent règlement en établissant la méthodologie pour calculer le nombre mensuel moyen de destinataires actifs du service dans l'Union aux fins du paragraphe 1 du présent article et de l'article 24, paragraphe 2, en veillant à ce que cette méthode tienne compte des évolutions du marché et de la technologie.

4. La Commission, après avoir consulté l'État membre d'établissement ou pris en compte les informations fournies par le coordinateur pour les services numériques de l'État membre d'établissement conformément à l'article 24, paragraphe 4, adopte une décision désignant comme une très grande plateforme en ligne ou un très grand moteur de recherche en ligne aux fins du présent règlement la plateforme en ligne ou le moteur de recherche en ligne dont le nombre mensuel moyen de destinataires actifs du service est égal ou supérieur au nombre visé au paragraphe 1 du présent article. La Commission prend cette décision sur la base des données communiquées par le fournisseur de la plateforme en ligne ou du moteur de recherche en ligne en vertu de l'article 24, paragraphe 2, des informations demandées en vertu de l'article 24, paragraphe 3, ou de toute autre information à la disposition de la Commission.

Le fait pour le fournisseur de la plateforme en ligne ou du moteur de recherche en ligne de ne pas se conformer à l'article 24, paragraphe 2, ou de ne pas donner suite à la demande du coordinateur pour les services numériques de l'État membre d'établissement ou de la Commission exprimée en vertu de l'article 24, paragraphe 3, n'empêche pas la Commission de désigner ce fournisseur comme un fournisseur d'une très grande plateforme en ligne ou d'un très grand moteur de recherche en ligne conformément au présent paragraphe.

Lorsque la Commission fonde sa décision sur d'autres informations dont elle dispose en vertu du premier alinéa du présent paragraphe, ou sur des informations complémentaires demandées en vertu de l'article 24, paragraphe 3, elle donne au fournisseur de la plateforme en ligne ou du moteur de recherche en ligne concerné un délai de dix jours ouvrables pour faire part de son point de vue sur ses conclusions préliminaires et sur son intention de désigner la plateforme en ligne ou le moteur de recherche en ligne comme une très grande plateforme en ligne ou un très grand moteur de recherche en ligne, respectivement. La Commission tient dûment compte du point de vue présenté par le fournisseur concerné.

Le fait pour le fournisseur de la plateforme en ligne ou du moteur de recherche en ligne concerné de ne pas faire part de son point de vue en vertu du troisième alinéa n'empêche pas la Commission de désigner cette plateforme en ligne ou ce moteur de recherche en ligne comme une très grande plateforme en ligne ou un très grand moteur de recherche en ligne, respectivement, sur la base des informations dont elle dispose.

5. La Commission met fin à cette désignation si, pendant une période ininterrompue d'un an, la plateforme en ligne ou le moteur de recherche en ligne n'a pas un nombre mensuel moyen de destinataires actifs supérieur ou égal au nombre visé au paragraphe 1.

6. La Commission notifie, sans retard injustifié, les décisions qu'elle prend en vertu des paragraphes 4 et 5 au fournisseur de la plateforme en ligne ou du moteur de recherche en ligne concerné, au comité et au coordinateur pour les services numériques de l'État membre d'établissement.

La Commission veille à ce que la liste des très grandes plateformes en ligne et des très grands moteurs de recherche en ligne désignés soit publiée au Journal officiel de l'Union européenne et tient cette liste à jour. Les obligations établies dans la présente section s'appliquent ou cessent de s'appliquer aux très grandes plateformes en ligne et aux très grands moteurs de recherche en ligne concernés quatre mois après la notification adressée au fournisseur concerné visée au premier alinéa.

Article 34 - Évaluation des risques

1. Les fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne recensent, analysent et évaluent de manière diligente tout risque systémique au sein de l'Union découlant de la conception ou du fonctionnement de leurs services et de leurs systèmes connexes, y compris des systèmes algorithmiques, ou de l'utilisation faite de leurs services.

Ils procèdent aux évaluations des risques au plus tard à la date d'application visée à l'article 33, paragraphe 6, deuxième alinéa, puis au moins une fois par an, et en tout état de cause avant de déployer des fonctionnalités susceptibles d'avoir une incidence critique sur les risques recensés en vertu du présent article. Cette évaluation des risques est spécifique à leurs services et proportionnée aux risques systémiques, de la gravité et de la probabilité desquels elle tient compte, et comprend les risques systémiques suivants:

a) la diffusion de contenus illicites par l'intermédiaire de leurs services;

b) tout effet négatif réel ou prévisible pour l'exercice des droits fondamentaux, en particulier le droit fondamental à la dignité humaine consacré à l'article 1er de la

Charte, au respect de la vie privée et familiale consacré à l'article 7 de la Charte, à la protection des données à caractère personnel consacré à l'article 8 de la Charte, à la liberté d'expression et d'information, y compris la liberté et le pluralisme des médias, consacré à l'article 11 de la Charte, et à la non-discrimination consacré à l'article 21 de la Charte, les droits fondamentaux relatifs aux droits de l'enfant consacrés à l'article 24 de la Charte et le droit fondamental à un niveau élevé de protection des consommateurs consacré à l'article 38 de la Charte;

c) tout effet négatif réel ou prévisible sur le discours civique, les processus électoraux et la sécurité publique;

d) tout effet négatif réel ou prévisible lié aux violences sexistes et à la protection de la santé publique et des mineurs et les conséquences négatives graves sur le bien-être physique et mental des personnes.

2. Lorsqu'ils procèdent à des évaluations des risques, les fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne examinent notamment si et comment les facteurs suivants influencent les risques systémiques visés au paragraphe 1 et en tiennent compte:

a) la conception de leurs systèmes de recommandation et de tout autre système algorithmique pertinent;

b) leurs systèmes de modération des contenus;

c) les conditions générales applicables et leur mise en application;

d) les systèmes de sélection et de présentation de la publicité;

e) les pratiques du fournisseur en matière de données.

Les évaluations examinent également si et comment les risques visés au paragraphe 1 sont influencés par la manipulation intentionnelle du service desdits fournisseurs, y compris par l'utilisation non authentique ou l'exploitation automatisée du service, ainsi que par l'amplification et la diffusion potentiellement rapide et à grande échelle de contenus illicites et d'informations incompatibles avec leurs conditions générales.

L'évaluation tient compte des aspects régionaux ou linguistiques spécifiques, y compris lorsqu'ils sont propres à un État membre.

3. Les fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne conservent les documents justificatifs des évaluations des risques pendant au moins trois ans après la réalisation de ces évaluations, et les communiquent à la Commission et au coordinateur pour les services numériques de l'État membre d'établissement, à leur demande.

Article 35 - Atténuation des risques

1. Les fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne mettent en place des mesures d'atténuation raisonnables, proportionnées et

efficaces, adaptées aux risques systémiques spécifiques recensés conformément à l'article 34, en tenant compte en particulier de l'incidence de ces mesures sur les droits fondamentaux. Ces mesures peuvent inclure, le cas échéant:

a) l'adaptation de la conception, des caractéristiques ou du fonctionnement de leurs services, y compris leurs interfaces en ligne;

b) l'adaptation de leurs conditions générales et de la mise en application de celles-ci;

c) l'adaptation des processus de modération des contenus, y compris la rapidité et la qualité du traitement des notifications relatives à des types spécifiques de contenus illicites et, le cas échéant, le retrait rapide des contenus qui ont fait l'objet d'une notification ou le blocage de l'accès à ces contenus, en particulier en ce qui concerne les discours haineux illégaux ou la cyberviolence, ainsi que l'adaptation des processus décisionnels pertinents et des ressources dédiées à la modération des contenus;

d) le test et l'adaptation de leurs systèmes algorithmiques, y compris leurs systèmes de recommandation;

e) l'adaptation de leurs systèmes de publicité et l'adoption de mesures ciblées destinées à limiter la présentation de publicités, ou à en adapter la présentation, en association avec le service fourni;

f) le renforcement des processus internes, des ressources, des tests, de la documentation ou de la surveillance d'une quelconque de leurs activités, notamment en ce qui concerne la détection des risques systémiques;

g) la mise en place d'une coopération avec les signaleurs de confiance, ou l'ajustement de cette coopération, conformément à l'article 22, ainsi que la mise en œuvre des décisions prises par les organes de règlement extrajudiciaire des litiges en vertu de l'article 21;

h) la mise en place d'une coopération avec d'autres fournisseurs de plateformes en ligne ou de moteurs de recherche en ligne, ou l'ajustement de cette coopération, sur la base des codes de conduite et des protocoles de crise visés aux articles 45 et 48, respectivement;

i) l'adoption de mesures de sensibilisation et l'adaptation de leur interface en ligne, afin de donner plus d'informations aux destinataires du service;

j) l'adoption de mesures ciblées visant à protéger les droits de l'enfant, y compris la vérification de l'âge et des outils de contrôle parental, ou des outils permettant d'aider les mineurs à signaler les abus ou à obtenir un soutien, s'il y a lieu;

k) le recours à un marquage bien visible pour garantir qu'un élément d'information, qu'il s'agisse d'une image, d'un contenu audio ou vidéo généré ou manipulé, qui ressemble nettement à des personnes, à des objets, à des lieux ou à d'autres entités ou événements réels, et apparaît à tort aux yeux d'une personne comme authentique ou digne de foi, est reconnaissable lorsqu'il est présenté sur leurs interfaces en ligne, et,

en complément, la mise à disposition d'une fonctionnalité facile d'utilisation permettant aux destinataires du service de signaler ce type d'information.

2. Le comité, en coopération avec la Commission, publie des rapports exhaustifs une fois par an. Ces rapports comprennent les éléments suivants:

a) le recensement et l'évaluation des risques systémiques les plus importants et récurrents signalés par les fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne ou recensés via d'autres sources d'informations, notamment celles fournies conformément aux articles 39, 40 et 42;

b) la définition de bonnes pratiques pour les fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne en vue de l'atténuation des risques systémiques recensés.

Ces rapports présentent les risques systémiques ventilés par État membre dans lequel ils sont survenus et pour l'ensemble de l'Union, s'il y a lieu.

3. La Commission, en coopération avec les coordinateurs pour les services numériques, peut publier des lignes directrices sur l'application du paragraphe 1 par rapport à des risques spécifiques, notamment en vue de présenter les bonnes pratiques et de recommander des mesures possibles, en tenant dûment compte des conséquences possibles des mesures sur les droits fondamentaux de toutes les parties concernées consacrés dans la Charte. Dans le cadre de l'élaboration de ces lignes directrices, la Commission organise des consultations publiques.

Article 36 - Mécanisme de réaction aux crises

1. En cas de crise, la Commission, sur recommandation du comité, peut adopter une décision exigeant qu'un ou plusieurs fournisseurs de très grandes plateformes en ligne ou de très grands moteurs de recherche entreprennent une ou plusieurs des actions suivantes:

a) évaluer si et, le cas échéant, comment et dans quelle mesure le fonctionnement et l'utilisation de leurs services contribuent de manière significative à une menace grave, telle qu'elle est visée au paragraphe 2, ou sont susceptibles de le faire;

b) déterminer et appliquer des mesures spécifiques, efficaces et proportionnées, telles que celles prévues à l'article 35, paragraphe 1, ou à l'article 48, paragraphe 2, pour prévenir, éliminer ou limiter toute contribution à la menace grave identifiée en vertu du point a) du présent paragraphe;

c) faire rapport à la Commission, à une date donnée ou à intervalles réguliers précisés dans la décision, sur les évaluations visées au point a), le contenu précis, la mise en œuvre et l'impact qualitatif et quantitatif des mesures spécifiques prises en application du point b), ainsi que sur tout autre aspect lié à ces évaluations ou mesures, précisé dans la décision.

Lorsqu'ils déterminent et appliquent des mesures conformément au point b) du présent paragraphe, le ou les fournisseurs de services tiennent dûment compte du caractère sérieux de la menace grave visée au paragraphe 2, de l'urgence des mesures ainsi que des répercussions réelles ou potentielles pour les droits et les intérêts légitimes de toutes les parties concernées,

y compris de l'éventualité que les mesures ne respectent pas les droits fondamentaux consacrés dans la Charte.

2. Aux fins du présent article, il y a lieu de conclure à une crise lorsque des circonstances extraordinaires entraînent une menace grave pour la sécurité publique ou la santé publique dans l'Union ou dans des parties importantes de l'Union.

3. Lorsqu'elle adopte la décision visée au paragraphe 1, la Commission veille à respecter l'ensemble des exigences suivantes:

a) les actions requises par la décision sont strictement nécessaires, justifiées et proportionnées, compte tenu notamment du caractère sérieux de la menace grave visée au paragraphe 2, de l'urgence des mesures ainsi que des répercussions réelles ou potentielles pour les droits et les intérêts légitimes de toutes les parties concernées, y compris de l'éventualité que les mesures ne respectent pas les droits fondamentaux consacrés dans la Charte;

b) décision définit une période raisonnable durant laquelle les mesures spécifiques visées au paragraphe 1, point b), doivent être prises, compte tenu notamment de l'urgence de ces mesures et du temps nécessaire pour leur élaboration et leur mise en œuvre;

c) les actions requises par la décision sont limitées à une durée n'excédant pas trois mois.

4. Après l'adoption de la décision visée au paragraphe 1, la Commission entreprend sans retard injustifié les actions suivantes:

a) notifier la décision aux fournisseurs qui en sont les destinataires;

b) rendre la décision publique; et

c) informer le comité de la décision, l'inviter à faire part de son point de vue sur celle-ci et le tenir informé de toute évolution ultérieure relative à la décision.

5. Le choix des mesures spécifiques à prendre en vertu du paragraphe 1, point b), et du paragraphe 7, deuxième alinéa, relève de la responsabilité du ou des fournisseurs visés par la décision de la Commission.

6. La Commission peut, de sa propre initiative ou à la demande du fournisseur, engager un dialogue avec ce dernier afin de déterminer si, à la lumière de la situation particulière du fournisseur, les mesures prévues ou appliquées, visées au paragraphe 1, point b), sont efficaces et proportionnées pour atteindre les objectifs poursuivis. En particulier, la Commission veille à ce que les mesures prises par le fournisseur de services au titre du paragraphe 1, point b), respectent les exigences visées au paragraphe 3, points a) et c).

7. La Commission contrôle l'application des mesures spécifiques prises en vertu de la décision visée au paragraphe 1 du présent article en s'appuyant sur les rapports visés au point c) dudit paragraphe et sur toute autre information pertinente, y compris les informations qu'elle peut demander en vertu de l'article 40 ou 67, en tenant compte de l'évolution de la crise. La Commission fait régulièrement rapport au comité sur ce contrôle, au moins une fois par mois.

Lorsque la Commission estime que les mesures spécifiques prévues ou appliquées en vertu du paragraphe 1, point b), ne sont pas efficaces ou proportionnées, elle peut, après consultation du comité, adopter une décision obligeant le fournisseur à réexaminer les mesures spécifiques qui ont été déterminées ou leur application.

8. S'il y a lieu, au regard de l'évolution de la crise, la Commission peut, sur recommandation du comité, modifier la décision visée au paragraphe 1 ou au paragraphe 7, deuxième alinéa, en:

a) Révoquant la décision et, s'il y a lieu, en demandant à la très grande plateforme en ligne ou au très grand moteur de recherche en ligne de cesser d'appliquer les mesures déterminées et mises en œuvre en vertu du paragraphe 1, point b), ou du paragraphe 7, deuxième alinéa, en particulier lorsque les motifs justifiant de telles mesures n'existent plus;

b) Prolongeant la période visée au paragraphe 3, point c), pour une durée n'excédant pas trois mois;

c) Prenant en compte l'expérience acquise dans l'application des mesures, notamment l'éventualité que les mesures ne respectent pas les droits fondamentaux consacrés par la Charte.

9. Les exigences des paragraphes 1 à 6 s'appliquent à la décision et à la modification de celle-ci visées au présent article.

10. La Commission tient le plus grand compte de la recommandation formulée par le comité en vertu du présent article.

11. Tous les ans après l'adoption de décisions conformément au présent article et, en tout état de cause, trois mois après la fin de la crise, la Commission fait rapport au Parlement européen et au Conseil sur l'application des mesures spécifiques prises en vertu desdites décisions.

Article 37- Audit indépendant

1. Les fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne font l'objet d'audits indépendants, à leurs propres frais et au minimum une fois par an, pour évaluer le respect des points suivants:

a) les obligations établies au chapitre III;

b) tout engagement pris en vertu des codes de conduite visés aux articles 45 et 46 et des protocoles de crise visés à l'article 48.

2. Les fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne accordent aux organisations effectuant les audits en vertu du présent article la coopération et l'assistance requises pour leur permettre de réaliser ces audits en temps utile, de manière efficace et efficiente, notamment en leur donnant accès à toutes les données et à tous les locaux pertinents et en répondant aux questions orales ou écrites qui leur sont posées.

Ils s'abstiennent d'entraver, d'influencer indûment ou de compromettre la réalisation de l'audit.

Ces audits garantissent un niveau adéquat de confidentialité et de secret professionnel en ce qui concerne les informations obtenues auprès des fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne et auprès de tiers dans le cadre des audits, y compris après la clôture de ces audits. Le respect de cette exigence ne porte toutefois pas atteinte à la réalisation des audits et aux autres dispositions du présent règlement, notamment celles concernant la transparence, la surveillance et l'exécution. S'il y a lieu, aux fins des rapports de transparence visés à l'article 42, paragraphe 4, le rapport d'audit et le rapport de mise en œuvre des recommandations d'audit visés aux paragraphes 4 et 6 du présent article sont accompagnés de versions qui ne contiennent pas d'informations qui pourraient raisonnablement être considérées comme confidentielles.

3. Les audits réalisés conformément au paragraphe 1 le sont par des organisations qui:

   a) sont indépendantes du fournisseur de très grandes plateformes en ligne ou de très grands moteurs de recherche en ligne concerné et de toute personne morale liée à ce fournisseur et ne sont pas en situation de conflit d'intérêts avec ceux-ci; en particulier:

      i) elles n'ont pas fourni de service, autre que d'audit, en rapport avec l'objet de l'audit au fournisseur de la très grande plateforme en ligne ou du très grand moteur de recherche en ligne concerné ni à une personne morale liée à ce fournisseur au cours des douze mois précédant le début de l'audit, et elles se sont engagées à ne leur fournir aucun service de ce type au cours des douze mois suivant la clôture de l'audit;

      ii) elles n'ont pas fourni de services d'audit en vertu du présent article au fournisseur de la très grande plateforme en ligne ou du très grand moteur de recherche en ligne concerné ni à une personne morale liée à ce fournisseur pendant une période supérieure à dix années consécutives;

      iii) elles ne réalisent pas l'audit en échange d'honoraires qui dépendent des résultats de cet audit;

   b) possèdent une expertise avérée dans le domaine de la gestion des risques, des compétences techniques et des capacités;

   c) démontrent une objectivité et une éthique professionnelle avérées, fondées notamment sur l'adhésion à des codes de pratique ou à des normes appropriées.

4. Les fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne veillent à ce que les organisations qui réalisent les audits établissent un rapport d'audit à la suite de chaque audit. Ce rapport motivé est établi par écrit et comporte au moins les éléments suivants:

   a) le nom, l'adresse et le point de contact du fournisseur de la très grande plateforme en ligne ou du très grand moteur de recherche en ligne faisant l'objet de l'audit et la période couverte;

b) le nom et l'adresse de la ou des organisations réalisant l'audit;

c) une déclaration d'intérêt;

d) une description des éléments spécifiques faisant l'objet de l'audit, et la méthodologie appliquée;

e) une description et une synthèse des principales conclusions tirées de l'audit;

f) une liste des tiers consultés dans le cadre de l'audit;

g) un avis d'audit sur le respect ou non par le fournisseur de la très grande plateforme en ligne ou du très grand moteur de recherche en ligne faisant l'objet de l'audit des obligations et des engagements visés au paragraphe 1, soit "positif", soit "positif et assorti de commentaires", soit "négatif";

h) lorsque l'avis d'audit n'est pas "positif", des recommandations opérationnelles sur les mesures spécifiques à prendre pour la mise en conformité ainsi que le calendrier recommandé à cet effet.

5. Lorsque l'organisation qui réalise l'audit n'a pas été en mesure de réaliser un audit à l'égard de certains éléments spécifiques ou d'émettre un avis d'audit sur la base de ses investigations, le rapport d'audit inclut une explication sur les circonstances et les raisons pour lesquelles ces éléments n'ont pas pu faire l'objet d'un audit.

6. Les fournisseurs de très grandes plateformes en ligne ou de très grands moteurs de recherche en ligne qui reçoivent un rapport d'audit qui n'est pas "positif" tiennent dûment compte des recommandations opérationnelles qui leur sont adressées en vue de prendre les mesures nécessaires à leur mise en œuvre. Dans le mois à compter de la réception de ces recommandations, ils adoptent un rapport de mise en œuvre des recommandations d'audit énonçant ces mesures. S'ils ne mettent pas en œuvre les recommandations opérationnelles, ils en fournissent les motifs dans le rapport de mise en œuvre des recommandations d'audit et exposent les mesures alternatives prises pour résoudre tout cas de manquement recensé.

7. La Commission est habilitée à adopter des actes délégués conformément à l'article 87 pour compléter le présent règlement en établissant les règles nécessaires à la réalisation des audits en vertu du présent article, notamment les règles nécessaires relatives aux étapes de la procédure, aux méthodes d'audit et aux modèles de rapport à utiliser pour les audits réalisés en vertu du présent article. Ces actes délégués tiennent compte de toute norme d'audit volontaire visée à l'article 44, paragraphe 1, point e).

Article 38 - Systèmes de recommandation

Outre les exigences prévues à l'article 27, les fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne qui utilisent des systèmes de recommandation proposent au moins une option pour chacun de leurs systèmes de recommandation qui ne repose pas sur du profilage, tel qu'il est défini à l'article 4, point 4), du règlement (UE) 2016/679.

Article 39 - Transparence renforcée de la publicité en ligne

1. Les fournisseurs de très grandes plateformes en ligne ou de très grands moteurs de recherche en ligne présentant de la publicité sur leurs interfaces en ligne tiennent et mettent à la disposition du public, dans une section spécifique de leur interface en ligne, à l'aide d'un outil de recherche fiable permettant d'effectuer des recherches multicritères et par l'intermédiaire d'interfaces de programme d'application, un registre contenant les informations visées au paragraphe 2, pour toute la période pendant laquelle ils présentent une publicité et jusqu'à un an après la dernière présentation de la publicité sur leurs interfaces en ligne. Ils veillent à ce que ce registre ne contienne aucune donnée à caractère personnel des destinataires du service auxquels la publicité a été ou aurait pu être présentée et s'efforcent, dans la mesure du raisonnable, de s'assurer de l'exactitude et de l'exhaustivité des informations.

2. Ce registre contient au moins toutes les informations suivantes:

   a) le contenu de la publicité, y compris le nom du produit, du service ou de la marque, ainsi que l'objet de la publicité;

   b) la personne physique ou morale pour le compte de laquelle la publicité est présentée;

   c) la personne physique ou morale qui a payé la publicité, si cette personne est différente de celle visée au point b);

   d) la période au cours de laquelle la publicité a été présentée;

   e) le fait que la publicité était ou non destinée à être présentée spécifiquement à un ou plusieurs groupes particuliers de destinataires du service et, dans l'affirmative, les principaux paramètres utilisés à cette fin, y compris, s'il y a lieu, les principaux paramètres utilisés pour exclure un ou plusieurs de ces groupes particuliers;

   f) les communications commerciales publiées sur les très grandes plateformes en ligne et déterminées en vertu de l'article 26, paragraphe 2;

   g) le nombre total de destinataires du service atteint et, le cas échéant, les nombres totaux ventilés par État membre pour le ou les groupes de destinataires que la publicité ciblait spécifiquement.

3. En ce qui concerne le paragraphe 2, points a), b) et c), lorsque le fournisseur d'une très grande plateforme en ligne ou d'un très grand moteur de recherche en ligne retire une publicité spécifique sur la base d'une allégation d'illégalité ou d'incompatibilité avec ses conditions générales ou rend impossible l'accès à cette publicité, le registre ne contient pas les informations visées dans lesdits points. Dans ce cas, le registre contient, pour la publicité spécifique concernée, les informations visées, selon le cas, à l'article 17, paragraphe 3, points a) à e), ou à l'article 9, paragraphe 2, point a) i).

La Commission peut, après consultation du comité, des chercheurs agréés visés à l'article 40 et du public, formuler des lignes directrices sur la structure, l'organisation et les fonctionnalités des registres visés dans le présent article.

Article 40- Accès aux données et contrôle des données

1. Les fournisseurs de très grandes plateformes en ligne ou de très grands moteurs de recherche en ligne donnent au coordinateur pour les services numériques de l'État membre d'établissement ou à la Commission, à leur demande motivée et dans un délai raisonnable spécifié dans cette demande, l'accès aux données nécessaires pour contrôler et évaluer le respect du présent règlement.

2. Les coordinateurs pour les services numériques et la Commission n'utilisent les données auxquelles ils ont eu accès conformément au paragraphe 1 qu'à des fins de contrôle et d'évaluation du respect du présent règlement et tiennent dûment compte des droits et intérêts des fournisseurs de très grandes plateformes en ligne ou de très grands moteurs de recherche en ligne et des destinataires du service concerné, y compris la protection des données à caractère personnel, la protection des informations confidentielles, en particulier les secrets d'affaires, et le maintien de la sécurité de leur service.

3. Aux fins du paragraphe 1, les fournisseurs de très grandes plateformes en ligne ou de très grands moteurs de recherche en ligne expliquent, à la demande du coordinateur pour les services numériques de l'État membre d'établissement ou de la Commission, la conception, la logique, le fonctionnement et la procédure de test de leurs systèmes algorithmiques, y compris leurs systèmes de recommandation.

4. Sur demande motivée du coordinateur pour les services numériques de l'État membre d'établissement, les fournisseurs de très grandes plateformes en ligne ou de très grands moteurs de recherche en ligne fournissent, dans un délai raisonnable spécifié dans la demande, l'accès aux données à des chercheurs agréés qui satisfont aux exigences énoncées au paragraphe 8 du présent article, à la seule fin de procéder à des recherches contribuant à la détection, au recensement et à la compréhension des risques systémiques dans l'Union tels qu'ils sont énoncés à l'article 34, paragraphe 1, ainsi qu'à l'évaluation du caractère adéquat, de l'efficacité et des effets des mesures d'atténuation des risques prises en vertu de l'article 35.

5. Dans les quinze jours suivant la réception d'une demande visée au paragraphe 4, les fournisseurs de très grandes plateformes en ligne ou de très grands moteurs de recherche en ligne peuvent demander au coordinateur pour les services numériques de l'État membre d'établissement de modifier la demande, lorsqu'ils considèrent ne pas être en mesure de fournir l'accès aux données demandées pour une des deux raisons suivantes:

a) ils n'ont pas accès aux données;

b) fournir l'accès aux données entraînera d'importantes vulnérabilités pour la sécurité de leur service ou la protection d'informations confidentielles, en particulier des secrets d'affaires.

6. Les demandes de modification en vertu du paragraphe 5 contiennent des propositions exposant une ou plusieurs solutions alternatives qui permettent de donner accès aux données demandées ou à d'autres données appropriées et suffisantes aux fins de la demande.

Le coordinateur pour les services numériques de l'État membre d'établissement se prononce sur la demande de modification dans les quinze jours et communique au fournisseur de la très

grande plateforme en ligne ou du très grand moteur de recherche en ligne sa décision et, le cas échéant, la demande modifiée et le nouveau délai pour donner suite à la demande.

7. Les fournisseurs de très grandes plateformes en ligne ou de très grands moteurs de recherche en ligne facilitent et fournissent l'accès aux données conformément aux paragraphes 1 et 4 par l'intermédiaire d'interfaces appropriées spécifiées dans la demande, y compris des bases de données en ligne ou des interfaces de programmation d'application.

8. Sur demande dûment motivée de chercheurs, le coordinateur pour les services numériques de l'État membre d'établissement accorde auxdits chercheurs le statut de chercheurs agréés pour la recherche spécifique visée dans la demande et adresse une demande motivée d'accès aux données au fournisseur de la très grande plateforme en ligne ou du très grand moteur de recherche en ligne conformément au paragraphe 4, lorsque les chercheurs démontrent qu'ils remplissent l'ensemble des conditions suivantes:

a) ils sont affiliés à un organisme de recherche tel qu'il est défini à l'article 2, point 1), de la directive (UE) 2019/790;

b) ils sont indépendants de tous intérêts commerciaux;

c) leur demande indique la source de financement des recherches;

d) ils sont à même de respecter les exigences spécifiques en matière de sécurité et de confidentialité des données correspondant à chaque demande ainsi que de protéger les données à caractère personnel, et ils décrivent dans leur demande les mesures techniques et organisationnelles appropriées qu'ils ont mis en place à cet effet;

e) dans leur demande, ils démontrent que leur accès aux données et les périodes d'accès demandées sont nécessaires et proportionnés aux fins poursuivies par leur recherche et que les résultats escomptés de cette recherche contribueront aux fins énoncées au paragraphe 4;

f) les activités de recherche prévues sont menées aux fins énoncées au paragraphe 4;

g) ils se sont engagés à mettre gratuitement à la disposition du public les résultats de leurs recherches dans un délai raisonnable après l'achèvement de celles-ci, sous réserve des droits et des intérêts des destinataires du service concerné, conformément au règlement (UE) 2016/679.

Dès réception de la demande visée au présent paragraphe, le coordinateur pour les services numériques de l'État membre d'établissement informe la Commission et le comité.

9. Les chercheurs peuvent également soumettre leur demande au coordinateur pour les services numériques de l'État membre de l'organisme de recherche auquel ils sont affiliés. Dès réception de la demande visée au présent paragraphe, le coordinateur pour les services numériques procède à une évaluation initiale visant à déterminer si les différents chercheurs remplissent toutes les conditions énoncées au paragraphe 8. Le coordinateur pour les services numériques concerné envoie la demande, accompagnée des documents justificatifs présentés par les chercheurs ainsi que de l'évaluation initiale, au coordinateur pour les services numériques de l'État membre d'établissement. Le coordinateur pour les services numériques

de l'État membre d'établissement adopte dans les meilleurs délais, une décision quant à l'octroi à un chercheur du statut de chercheur agréé.

Tout en tenant dûment compte de l'évaluation initiale fournie, la décision finale d'octroyer à un chercheur le statut de chercheur agréé relève de la compétence du coordinateur pour les services numériques de l'État membre d'établissement, conformément au paragraphe 8.

10. Le coordinateur pour les services numériques ayant octroyé le statut de chercheur agréé et adressé la demande motivée d'accès aux données aux fournisseurs de très grandes plateformes en ligne ou de très grands moteurs de recherche en ligne en faveur d'un chercheur agréé, adopte une décision mettant fin à cet accès s'il constate, à la suite d'une enquête menée soit de sa propre initiative, soit sur la base d'informations reçues de tiers, que le chercheur agréé ne remplit plus les conditions établies au paragraphe 8, et informe le fournisseur de la très grande plateforme en ligne ou du très grand moteur de recherche en ligne concerné de sa décision. Avant de mettre fin à l'accès, le coordinateur pour les services numériques donne au chercheur agréé la possibilité de réagir aux conclusions de l'enquête et à son intention de mettre fin à l'accès.

11. Les coordinateurs pour les services numériques de l'État membre d'établissement communiquent au comité les noms et les coordonnées des personnes physiques ou des entités auxquelles ils ont accordé le statut de chercheur agréé conformément au paragraphe 8, ainsi que l'objet de la recherche pour laquelle la demande a été soumise, ou l'informent qu'ils ont mis fin à l'accès aux données conformément au paragraphe 10 si c'est le cas.

12. Les fournisseurs de très grandes plateformes en ligne ou de très grands moteurs de recherche en ligne donnent accès, sans retard injustifié, aux données, y compris, lorsque cela est techniquement possible, aux données en temps réel, à condition que ces données soient publiquement accessibles sur leur interface en ligne aux chercheurs, y compris ceux qui sont affiliés à des organismes et des associations à but non lucratif, qui remplissent les conditions énoncées au paragraphe 8, points b), c), d) et e), et qui utilisent les données uniquement à des fins de recherches contribuant à la détection, à la détermination et à la compréhension des risques systémiques dans l'Union en vertu de l'article 34, paragraphe 1.

13. Après consultation du comité, la Commission adopte des actes délégués qui complètent le présent règlement en établissant les conditions techniques dans lesquelles les fournisseurs de très grandes plateformes en ligne ou de très grands moteurs de recherche en ligne partagent des données en vertu des paragraphes 1 et 4 et les fins auxquelles ces données peuvent être utilisées. Ces actes délégués établissent les conditions spécifiques dans lesquelles un tel partage de données avec des chercheurs peut avoir lieu en conformité avec le règlement (UE) 2016/679, ainsi que les indicateurs objectifs pertinents, les procédures et, si nécessaire, les mécanismes consultatifs indépendants à l'appui du partage de données, en tenant compte des droits et des intérêts des fournisseurs de très grandes plateformes en ligne ou de très grands moteurs de recherche en ligne et des destinataires du service concernés, y compris la protection des informations confidentielles, notamment les secrets d'affaires, et en préservant la sécurité de leur service.

Article 41- Fonction de contrôle de la conformité

1. Les fournisseurs de très grandes plateformes en ligne ou de très grands moteurs de recherche en ligne créent une fonction de contrôle de la conformité, qui est indépendante de

leurs fonctions opérationnelles et composée d'un ou de plusieurs responsables de la conformité, y compris le responsable de la fonction de contrôle de la conformité. La fonction de contrôle de la conformité dispose d'une autorité, d'une taille et de ressources suffisantes, ainsi que de l'accès à l'organe de direction du fournisseur de la très grande plateforme en ligne ou du très grand moteur de recherche en ligne nécessaire pour contrôler le respect du présent règlement par ce fournisseur.

2. L'organe de direction du fournisseur de la très grande plateforme en ligne ou du très grand moteur de recherche en ligne veille à ce que les responsables de la conformité disposent des qualifications professionnelles, des connaissances, de l'expérience et des aptitudes nécessaires pour mener à bien les tâches visées au paragraphe 3.

L'organe de direction du fournisseur de la très grande plateforme en ligne ou du très grand moteur de recherche en ligne veille à ce que le responsable de la fonction de contrôle de la conformité soit un cadre supérieur indépendant chargé spécifiquement de la fonction de contrôle de la conformité.

Le responsable de la fonction de contrôle de la conformité fait directement rapport à l'organe de direction du fournisseur de la très grande plateforme en ligne ou du très grand moteur de recherche en ligne et peut faire part de ses préoccupations auprès de cet organe et l'avertir lorsque les risques visés à l'article 34 ou le non-respect du présent règlement affectent ou sont susceptibles d'affecter le fournisseur de la très grande plateforme en ligne ou du très grand moteur de recherche en ligne concerné, sans préjudice des responsabilités de l'organe de direction dans ses fonctions de surveillance et de gestion.

Le responsable de la fonction de contrôle de la conformité n'est pas démis de ses fonctions sans l'accord préalable de l'organe de direction du fournisseur de la très grande plateforme en ligne ou du très grand moteur de recherche en ligne.

3. Les responsables de la conformité sont investis des tâches suivantes:

a) coopérer avec le coordinateur pour les services numériques de l'État membre d'établissement et la Commission aux fins du présent règlement;

b) veiller à ce que tous les risques visés à l'article 34 soient recensés et dûment notifiés et à ce que des mesures d'atténuation des risques raisonnables, proportionnées et efficaces soient prises conformément à l'article 35;

c) organiser et superviser les activités du fournisseur de la très grande plateforme en ligne ou du très grand moteur de recherche en ligne en lien avec l'audit indépendant en vertu de l'article 37;

d) informer et conseiller la direction et les employés du fournisseur de la très grande plateforme en ligne ou du très grand moteur de recherche en ligne au sujet des obligations pertinentes au titre du présent règlement;

e) contrôler le respect, par le fournisseur de la très grande plateforme en ligne ou du très grand moteur de recherche en ligne, de ses obligations au titre du présent règlement;

f) le cas échéant, contrôler le respect, par le fournisseur de la très grande plateforme en ligne ou du très grand moteur de recherche en ligne, des engagements qu'il a pris au titre des codes de conduite en vertu des articles 45 et 46 ou des protocoles de crise en vertu de l'article 48.

4. Les fournisseurs de très grandes plateformes en ligne ou de très grands moteurs de recherche en ligne communiquent le nom et les coordonnées du responsable de la fonction de contrôle de la conformité au coordinateur pour les services numériques de l'État membre d'établissement et à la Commission.

5. L'organe de direction du fournisseur de la très grande plateforme en ligne ou du très grand moteur de recherche en ligne détermine et supervise la mise en œuvre des dispositifs de gouvernance du fournisseur qui garantissent l'indépendance de la fonction de contrôle de la conformité, y compris la répartition des responsabilités au sein de l'organisation du fournisseur de la très grande plateforme en ligne ou du très grand moteur de recherche en ligne, la prévention des conflits d'intérêts et la bonne gestion des risques systémiques recensés conformément à l'article 34, et est tenu de rendre compte de cette mise en œuvre.

6. L'organe de direction approuve et réexamine périodiquement, au moins une fois par an, les stratégies et les politiques relatives à la prise en compte, à la gestion, au suivi et à l'atténuation des risques recensés conformément à l'article 34 auxquels la très grande plateforme en ligne ou le très grand moteur de recherche en ligne est ou pourrait être exposé.

7. L'organe de direction consacre suffisamment de temps à l'examen des mesures liées à la gestion des risques. Il participe activement aux décisions relatives à la gestion des risques et veille à ce que des ressources adéquates soient allouées à la gestion des risques recensés conformément à l'article 34.

Article 42 - Obligations en matière de rapports de transparence

1. Les fournisseurs de très grandes plateformes en ligne ou de très grands moteurs de recherche en ligne publient les rapports visés à l'article 15 au plus tard deux mois à compter de la date d'application visée à l'article 33, paragraphe 6, deuxième alinéa, puis au moins tous les six mois.

2. Outre les informations visées à l'article 15 et à l'article 24, paragraphe 1, les rapports visés au paragraphe 1 du présent article, publiés par les fournisseurs de très grandes plateformes en ligne, précisent:

a) les ressources humaines que le fournisseur de très grandes plateformes en ligne consacre à la modération des contenus en ce qui concerne le service proposé dans l'Union, ventilées par langue officielle concernée des États membres, y compris pour le respect des obligations énoncées aux articles 16 et 22 et de celles énoncées à l'article 20;

b) les qualifications et les connaissances linguistiques des personnes accomplissant les activités visées au point a) ainsi que la formation et l'accompagnement qui leur sont apportés;

c) les indicateurs de précision et les informations y afférentes visés à l'article 15, paragraphe 1, point e), ventilés par langue officielle des États membres.

Les rapports sont publiés dans au moins une des langues officielles des États membres.

3. En plus des informations visées à l'article 24, paragraphe 2, les fournisseurs de très grandes plateformes en ligne ou de très grands moteurs de recherche en ligne incluent, dans les rapports visés au paragraphe 1 du présent article, des informations sur le nombre mensuel moyen de destinataires du service dans chaque État membre.

4. Les fournisseurs de très grandes plateformes en ligne ou de très grands moteurs de recherche en ligne transmettent au coordinateur pour les services numériques de l'État membre d'établissement et à la Commission, sans retard injustifié dès leur achèvement, et mettent à la disposition du public au plus tard trois mois après la réception de chaque rapport d'audit conformément à l'article 37, paragraphe 4:

a) un rapport exposant les résultats de l'évaluation des risques au titre de l'article 34;

b) les mesures spécifiques d'atténuation mises en place en vertu de l'article 35, paragraphe 1;

c) le rapport d'audit prévu à l'article 37, paragraphe 4;

d) le rapport de mise en œuvre des recommandations d'audit prévu à l'article 37, paragraphe 6;

e) s'il y a lieu, les informations relatives aux consultations menées par le fournisseur pour les besoins des évaluations des risques et de la conception des mesures d'atténuation des risques.

5. Lorsqu'un fournisseur de très grandes plateformes en ligne ou de très grands moteurs de recherche en ligne considère que la publication d'informations conformément au paragraphe 4 pourrait mener à la divulgation d'informations confidentielles de ce fournisseur ou des destinataires du service, entraîner d'importantes vulnérabilités pour la sécurité de son service, porter atteinte à la sécurité publique ou nuire aux destinataires, il peut retirer ces informations des rapports accessibles au public. Dans ce cas, le fournisseur transmet les rapports complets au coordinateur pour les services numériques de l'État membre d'établissement et à la Commission, accompagnés d'un exposé des motifs pour lesquels ces informations ont été retirées des rapports accessibles au public.

Article 43- Redevance de surveillance

1. La Commission perçoit auprès des fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne une redevance de surveillance annuelle au moment de leur désignation en vertu de l'article 33.

2. Le montant total de la redevance de surveillance annuelle couvre les frais estimés que doit engager la Commission pour mener à bien les missions de surveillance que lui confie le présent règlement, en particulier les frais afférents aux désignations prévues à l'article 33, à la création, à la maintenance et au fonctionnement de la base de données visée à l'article 24,

paragraphe 5, et au système de partage d'informations visé à l'article 85, aux saisines visées à l'article 59, à l'appui apporté au comité conformément à l'article 62 et aux missions de surveillance visées à l'article 56 et au chapitre IV, section 4.

3. Une redevance de surveillance est perçue chaque année auprès des fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne pour chaque service pour lequel ils ont été désignés en vertu de l'article 33.

La Commission adopte des actes d'exécution fixant le montant de la redevance de surveillance annuelle pour chaque fournisseur de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne. Lorsqu'elle adopte ces actes d'exécution, la Commission applique la méthode établie dans l'acte délégué visé au paragraphe 4 du présent article et respecte les principes énoncés au paragraphe 5 du présent article. Ces actes d'exécution sont adoptés en conformité avec la procédure de consultation visée à l'article 88.

4. La Commission adoptes des actes délégués conformément à l'article 87 fixant, dans le détail, la méthode et les procédures à employer pour:

a) la détermination des frais estimés visés au paragraphe 2;

b) la détermination des redevances de surveillance annuelles individuelles visées au paragraphe 5, points b) et c);

c) la détermination du plafond global défini au paragraphe 5, point c); et

d) les modalités nécessaires pour effectuer les paiements.

Lorsqu'elle adopte ces actes délégués, la Commission respecte les principes énoncés au paragraphe 5 du présent article.

5. L'acte d'exécution visé au paragraphe 3 et l'acte délégué visé au paragraphe 4 respectent les principes suivants:

a) l'estimation du montant total de la redevance de surveillance annuelle tient compte des frais engagés lors de l'exercice précédent;

b) la redevance de surveillance annuelle est proportionnelle au nombre mensuel moyen de destinataires actifs dans l'Union de chaque très grande plateforme en ligne ou de chaque très grand moteur de recherche en ligne désigné en vertu de l'article 33;

c) le montant total de la redevance de surveillance annuelle perçue auprès d'un fournisseur donné de très grandes plateformes en ligne ou de très grands moteurs de recherche ne dépasse en aucun cas 0,05 % de son résultat net mondial annuel de l'exercice précédent.

6. Les redevances de surveillance annuelles individuelles perçues conformément au paragraphe 1 du présent article constituent des recettes affectées externes conformément à l'article 21, paragraphe 5, du règlement (UE, Euratom) 2018/1046 du Parlement européen et du Conseil (41).

7. La Commission présente chaque année au Parlement européen et au Conseil un rapport sur le montant total des frais engagés pour l'accomplissement des missions qui lui incombent au titre du présent règlement et sur le montant total des redevances de surveillance annuelles individuelles perçues lors de l'exercice précédent.

SECTION 6

Autres dispositions concernant les obligations de diligence

Article 44 - Normes

1. La Commission consulte le comité et soutient et encourage le développement ainsi que la mise en œuvre de normes volontaires établies par les organismes de normalisation européens et internationaux pertinents, au minimum pour les aspects suivants:

a) la soumission électronique des notifications au titre de l'article 16;

b) les modèles et les normes de conception et de procédure à employer pour communiquer avec les destinataires du service de manière conviviale sur les restrictions résultant des conditions générales et les modifications qui leur sont apportées;

c) la soumission électronique des notifications par les signaleurs de confiance au titre de l'article 22, y compris par l'intermédiaire d'interfaces de programme d'application;

d) les interfaces spécifiques, y compris les interfaces de programme d'application, visant à faciliter le respect des obligations établies aux articles 39 et 40;

e) l'audit des très grandes plateformes en ligne et des très grands moteurs de recherche en ligne au titre de l'article 37;

f) l'interopérabilité des registres de publicités visés à l'article 39, paragraphe 2;

g) la transmission de données entre les intermédiaires de publicité aux fins des obligations de transparence en vertu de l'article 26, paragraphe 1, points b), c) et d);

h) les mesures techniques permettant de satisfaire aux obligations relatives à la publicité contenues dans le présent règlement, y compris les obligations relatives aux marquages bien visibles à employer pour les publicités et les communications commerciales visées à l'article 26;

i) les interfaces de choix et la présentation des informations sur les principaux paramètres des différents types de systèmes de recommandation, conformément aux articles 27 et 38;

j) les normes applicables aux mesures ciblées destinées à protéger les mineurs en ligne.

2. La Commission soutient la mise à jour des normes à la lumière des évolutions technologiques et du comportement des destinataires des services en question. Les

informations pertinentes concernant la mise à jour des normes sont mises à la disposition du public et facilement accessibles.

Article 45 - Codes de conduite

1. La Commission et le comité encouragent et facilitent l'élaboration de codes de conduite volontaires au niveau de l'Union pour contribuer à la bonne application du présent règlement, en tenant compte notamment des difficultés spécifiques à surmonter pour faire face à différents types de contenus illicites et de risques systémiques, conformément au droit de l'Union notamment en matière de concurrence et de protection des données à caractère personnel.

2. Lorsqu'un risque systémique important au sens de l'article 34, paragraphe 1, apparaît et concerne plusieurs très grandes plateformes en ligne ou très grands moteurs de recherche en ligne, la Commission peut inviter les fournisseurs des très grandes plateformes en ligne concernées ou les fournisseurs des très grands moteurs de recherche en ligne concernés, et d'autres fournisseurs de très grandes plateformes en ligne, de très grands moteurs de recherche en ligne, de plateformes en ligne et d'autres services intermédiaires, selon qu'il convient, ainsi que les autorités compétentes concernées, des organisations de la société civile et d'autres parties prenantes concernées, à participer à l'élaboration de codes de conduite, y compris en formulant des engagements portant sur l'adoption de mesures spécifiques d'atténuation des risques, ainsi que d'un cadre pour la présentation de rapports réguliers concernant les mesures adoptées et leurs résultats.

3. En donnant effet aux paragraphes 1 et 2, la Commission et le comité, ainsi que d'autres organes s'il y a lieu, s'efforcent de garantir que les codes de conduite établissent clairement leurs objectifs spécifiques, contiennent des indicateurs clés de performance pour mesurer la réalisation de ces objectifs et tiennent dûment compte des besoins et des intérêts de toutes les parties intéressées, et en particulier des citoyens, au niveau de l'Union. La Commission et le comité s'efforcent également de garantir que les participants communiquent régulièrement à la Commission et à leurs coordinateurs pour les services numériques de l'État membre d'établissement respectifs les mesures qu'ils adoptent et leurs résultats, mesurés par rapport aux indicateurs clés de performance que les codes de conduite contiennent. Les indicateurs de performance clés et les engagements en matière de présentation de rapports tiennent compte des différences de taille et de capacité entre les différents participants.

4. La Commission et le comité évaluent si les codes de conduite satisfont aux objectifs spécifiés aux paragraphes 1 et 3, et contrôlent et évaluent régulièrement la réalisation de leurs objectifs, en tenant compte des indicateurs clés de performance qu'ils pourraient contenir. Ils publient leurs conclusions.

La Commission et le comité encouragent et facilitent également le réexamen régulier et l'adaptation des codes de conduite.

En cas de non-respect systématique des codes de conduite, la Commission et le comité peuvent inviter les signataires desdits codes à prendre les mesures qui s'imposent.

Article 46 - Codes de conduite pour la publicité en ligne

1. La Commission encourage et facilite l'élaboration de codes de conduite volontaires au niveau de l'Union par les fournisseurs de plateformes en ligne et d'autres fournisseurs de services pertinents, tels que les fournisseurs de services intermédiaires de publicité en ligne, d'autres acteurs participant à la chaîne de valeur de la publicité programmatique, ou les organisations représentant les destinataires du service et les organisations de la société civile ou les autorités compétentes, en vue de contribuer à une transparence accrue pour les acteurs de la chaîne de valeur de la publicité en ligne, au-delà des exigences des articles 26 et 39.

2. La Commission s'efforce de garantir que les codes de conduite favorisent la transmission efficace des informations, dans le plein respect des droits et intérêts de toutes les parties concernées, ainsi qu'un environnement compétitif, transparent et équitable pour la publicité en ligne, conformément au droit de l'Union et au droit national, notamment en matière de concurrence et de protection de la vie privée et des données à caractère personnel. La Commission s'efforce de garantir que les codes de conduite portent au minimum sur:

a) la transmission des informations détenues par les fournisseurs de services intermédiaires de publicité en ligne aux destinataires du service en ce qui concerne les exigences établies à l'article 26, paragraphe 1, points b), c) et d);

b) la transmission des informations détenues par les fournisseurs de services intermédiaires de publicité en ligne aux registres en vertu de l'article 39;

c) des informations utiles sur la monétisation des données.

3. La Commission encourage l'élaboration des codes de conduite pour le 18 février 2025 et leur application pour le 18 août 2025.

4. La Commission encourage tous les acteurs de la chaîne de valeur de la publicité en ligne visés au paragraphe 1 à adhérer aux engagements formulés dans les codes de conduite et à les respecter.

Article 47 - Codes de conduite relatifs à l'accessibilité

1. La Commission encourage et facilite l'élaboration de codes de conduite au niveau de l'Union, avec la participation des fournisseurs de plateformes en ligne et d'autres fournisseurs de services pertinents, les organisations représentant les destinataires du service et les organisations de la société civile ou les autorités compétentes afin de promouvoir la participation pleine et effective des personnes handicapées, sur un pied d'égalité, en améliorant leur accès aux services en ligne qui, du fait de leur conception initiale ou de leur adaptation ultérieure, répondent aux besoins spécifiques des personnes handicapées.

2. La Commission s'efforce de garantir que les codes de conduite poursuivent l'objectif d'assurer l'accessibilité de ces services, conformément au droit de l'Union et au droit national, afin de garantir une utilisation prévisible optimale par les personnes handicapées de ces services. La Commission s'efforce de garantir que les codes de conduite visent à atteindre au moins les objectifs suivants:

a) concevoir et adapter les services pour qu'ils soient accessibles aux personnes handicapées en les rendant perceptibles, utilisables, compréhensibles et robustes;

b) expliquer comment les services répondent aux exigences d'accessibilité applicables et mettre ces informations à la disposition du public d'une manière accessible aux personnes handicapées;

c) mettre les informations, les formulaires et les mesures fournis en vertu du présent règlement à disposition de manière à ce qu'ils soient faciles à trouver, faciles à comprendre et accessibles aux personnes handicapées.

3. La Commission encourage l'élaboration des codes de conduite au plus tard le 18 février 2025 et leur application au plus tard le 18 août 2025.

Article 48 - Protocoles de crise

1. Le comité peut recommander à la Commission de lancer l'élaboration, conformément aux paragraphes 2, 3 et 4, de protocoles de crise volontaires pour faire face aux situations de crise. Ces situations sont strictement limitées à des circonstances extraordinaires affectant la sécurité publique ou la santé publique.

2. La Commission encourage et facilite la participation des fournisseurs de très grandes plateformes en ligne, de très grands moteurs de recherche en ligne et, le cas échéant, les fournisseurs d'autres plateformes en ligne ou d'autres moteurs de recherche en ligne, à l'élaboration, aux essais et à l'application de ces protocoles de crise. La Commission s'efforce de garantir que ces protocoles de crise comprennent une ou plusieurs des mesures suivantes:

a) afficher de manière bien visible les informations relatives à la situation de crise fournies par les autorités des États membres ou au niveau de l'Union ou, en fonction du contexte de la crise, par d'autres organes fiables concernés;

b) veiller à ce que le fournisseur de services intermédiaires désigne un point de contact spécifique pour la gestion des crises; le cas échéant, il peut s'agir du point de contact électronique visé à l'article 11 ou, dans le cas de fournisseurs de très grandes plateformes en ligne ou de très grands moteurs de recherche en ligne, du responsable de la conformité visé à l'article 41;

c) le cas échéant, adapter les ressources dédiées au respect des obligations établies aux articles 16, 20, 22, 23 et 35 aux besoins découlant de la situation de crise.

3. La Commission associe, selon qu'il convient, les autorités des États membres et peut également associer les organes et organismes de l'Union à l'élaboration, aux essais et à la supervision de l'application des protocoles de crise. La Commission peut également, si nécessaire et selon qu'il convient, associer des organisations de la société civile ou d'autres organisations pertinentes à l'élaboration des protocoles de crise.

4. La Commission s'efforce de garantir que les protocoles de crise établissent clairement l'ensemble des éléments suivants:

a) les paramètres spécifiques utilisés pour déterminer ce qui constitue la circonstance extraordinaire spécifique à laquelle le protocole de crise entend répondre, ainsi que les objectifs qu'il poursuit;

b) le rôle de chacun des participants et les mesures qu'ils doivent mettre en place à titre préparatoire et en cas d'activation du protocole de crise;

c) une procédure claire pour déterminer le moment auquel le protocole de crise doit être activé;

d) une procédure claire pour déterminer la période au cours de laquelle les mesures à prendre en cas d'activation du protocole de crise doivent être prises, qui est strictement limitée à ce qui est nécessaire pour faire face aux circonstances extraordinaires spécifiques concernées;

e) les mesures de sauvegarde contre les effets négatifs éventuels sur l'exercice des droits fondamentaux consacrés dans la Charte, en particulier la liberté d'expression et d'information et le droit à la non-discrimination;

f) une procédure pour communiquer publiquement sur les mesures adoptées, leur durée et leurs résultats lorsque la situation de crise a pris fin.

5. Si la Commission considère qu'un protocole de crise ne répond pas de manière efficace à une situation de crise, ou ne sauvegarde pas l'exercice des droits fondamentaux comme prévu au paragraphe 4, point e), elle demande aux participants de réviser le protocole de crise, notamment en prenant des mesures complémentaires.

CHAPITRE IV

MISE EN ŒUVRE, COOPÉRATION, SANCTIONS ET EXÉCUTION

SECTION 1

Autorités compétentes et coordinateurs nationaux pour les services numériques

Article 49 - Autorités compétentes et coordinateurs pour les services numériques

1. Les États membres désignent une ou plusieurs autorités compétentes comme responsables de la surveillance des fournisseurs de services intermédiaires et de l'exécution du présent règlement (ci-après dénommées les "autorités compétentes").

2. Les États membres désignent une des autorités compétentes comme leur coordinateur pour les services numériques. Le coordinateur pour les services numériques est responsable de toutes les questions en lien avec la surveillance et l'exécution du présent règlement dans cet État membre, sauf si l'État membre concerné a assigné certaines missions ou certains secteurs spécifiques à d'autres autorités compétentes. Le coordinateur pour les services numériques a, en tout état de cause, la responsabilité d'assurer la coordination au niveau national vis-à-vis de ces questions et de contribuer à une surveillance et une exécution efficaces et cohérentes du présent règlement dans toute l'Union.

À cette fin, les coordinateurs pour les services numériques coopèrent entre eux, ainsi qu'avec les autres autorités compétentes nationales, le comité et la Commission, sans préjudice de la possibilité dont disposent les États membres de prévoir des mécanismes de coopération et des

échanges de vues réguliers entre les coordinateurs pour les services numériques et d'autres autorités nationales, lorsque cela présente de l'intérêt pour l'exécution de leurs missions respectives.

Lorsqu'un État membre désigne une ou plusieurs autorités compétentes en plus du coordinateur pour les services numériques, il veille à ce que les missions respectives de ces autorités et du coordinateur pour les services numériques soient clairement définies et à ce qu'ils coopèrent de manière étroite et efficace dans l'exécution de leurs missions.

3. Les États membres désignent les coordinateurs pour les services numériques au plus tard le 17 février 2024.

Les États membres rendent publics et communiquent à la Commission et au comité le nom de leur autorité compétente désignée en tant que coordinateur pour les services numériques, ainsi que des informations sur la manière dont il peut être contacté. L'État membre concerné communique à la Commission et au comité le nom des autres autorités compétentes visées au paragraphe 2 ainsi que leurs missions respectives.

4. Les dispositions applicables aux coordinateurs pour les services numériques énoncées aux articles 50, 51 et 56 s'appliquent également aux autres autorités compétentes désignées par les États membres en vertu du paragraphe 1 du présent article.

Article 50

Exigences applicables aux coordinateurs pour les services numériques

1. Les États membres veillent à ce que les coordinateurs pour les services numériques accomplissent leurs missions au titre du présent règlement de manière impartiale, transparente et en temps utile. Les États membres veillent à ce que leurs coordinateurs pour les services numériques disposent de toutes les ressources nécessaires à l'accomplissement de leurs missions, y compris des ressources techniques, financières et humaines suffisantes pour surveiller correctement tous les fournisseurs de services intermédiaires relevant de leur compétence. Chaque État membre veille à ce que son coordinateur pour les services numériques dispose d'une autonomie suffisante dans la gestion de son budget dans les limites globales du budget, afin de ne pas porter atteinte à l'indépendance du coordinateur pour les services numériques.

2. Lorsqu'ils accomplissent leurs missions et exercent leurs pouvoirs conformément au présent règlement, les coordinateurs pour les services numériques agissent en toute indépendance. Ils restent libres de toute influence extérieure, directe ou indirecte, et ne sollicitent ni n'acceptent aucune instruction d'aucune autre autorité publique ou partie privée.

3. Le paragraphe 2 du présent article est sans préjudice des missions incombant aux coordinateurs pour les services numériques dans le cadre du système de surveillance et d'exécution prévu dans le présent règlement et de la coopération avec les autres autorités compétentes conformément à l'article 49, paragraphe 2. Le paragraphe 2 du présent article n'empêche pas l'exercice d'un contrôle juridictionnel et est également sans préjudice d'exigences proportionnées en matière de responsabilisation en ce qui concerne les activités générales des coordinateurs pour les services numériques, par exemple en ce qui concerne les

dépenses financières ou les rapports à communiquer aux parlements nationaux, à condition que ces exigences ne portent pas atteinte à la réalisation des objectifs du présent règlement.

Article 51- Pouvoirs des coordinateurs pour les services numériques

1. Lorsque cela est nécessaire à l'accomplissement de leurs missions au titre du présent règlement, les coordinateurs pour les services numériques sont investis des pouvoirs d'enquête suivants à l'égard de la conduite des fournisseurs de services intermédiaires relevant de la compétence de leur État membre:

a) le pouvoir d'exiger de ces fournisseurs, ainsi que de toute autre personne agissant pour les besoins de son activité commerciale, industrielle, artisanale ou libérale et raisonnablement susceptible d'être au courant d'informations relatives à une infraction présumée au présent règlement, y compris les organisations qui réalisent les audits visés à l'article 37 et à l'article 75, paragraphe 2, qu'ils fournissent ces informations dans les meilleurs délais;

b) le pouvoir de procéder à des inspections dans tout local utilisé par ces fournisseurs ou ces personnes pour les besoins de leur activité commerciale, industrielle, artisanale ou libérale, ou de demander à une autorité judiciaire de leur État membre d'ordonner une telle inspection, ou de demander à d'autres autorités publiques de procéder à une telle inspection, afin d'examiner, de saisir, de prendre ou d'obtenir des copies d'informations relatives à une infraction présumée sous quelque forme et sur quelque support de stockage que ce soit;

c) le pouvoir de demander à tout membre du personnel ou représentant de ces fournisseurs ou de ces personnes de fournir des explications sur toute information relative à une infraction présumée et d'enregistrer leurs réponses avec leur consentement à l'aide de tout moyen technique.

2. Lorsque cela est nécessaire à l'accomplissement de leurs missions au titre du présent règlement, les coordinateurs pour les services numériques sont investis des pouvoirs d'exécution suivants à l'égard des fournisseurs de services intermédiaires relevant de la compétence de leur État membre:

a) le pouvoir d'accepter les engagements proposés par ces fournisseurs pour se conformer au présent règlement et de rendre ces engagements contraignants;

b) le pouvoir d'ordonner la cessation des infractions et, le cas échéant, d'imposer des mesures correctives proportionnées à l'infraction et nécessaires pour faire cesser effectivement l'infraction, ou de demander à une autorité judiciaire de leur État membre d'y procéder;

c) le pouvoir d'imposer des amendes, ou de demander à une autorité judiciaire de leur État membre d'y procéder, conformément à l'article 52 pour non-respect du présent règlement, y compris de toute injonction d'enquête émise en vertu du paragraphe 1 du présent article;

d) le pouvoir d'imposer une astreinte, ou de demander à une autorité judiciaire de leur État membre d'y procéder, conformément à l'article 52 pour qu'il soit mis fin à une

infraction conformément à une injonction émise en vertu du point b) du présent alinéa ou pour non-respect de toute injonction d'enquête émise en vertu du paragraphe 1 du présent article;

e) le pouvoir d'adopter des mesures provisoires ou de demander à l'autorité judiciaire nationale compétente de leur État membre d'y procéder afin d'éviter le risque de préjudice grave.

En ce qui concerne le premier alinéa, points c) et d), les coordinateurs pour les services numériques disposent également des pouvoirs d'exécution prévus dans ces points à l'égard des autres personnes visées au paragraphe 1 pour non-respect de toute injonction qui leur est adressée en vertu dudit paragraphe. Ils n'exercent ces pouvoirs d'exécution qu'après avoir fourni à ces autres personnes, en temps utile, toutes les informations pertinentes en lien avec ces injonctions, y compris le délai applicable, les amendes ou astreintes susceptibles d'être imposées en cas de non-respect et les possibilités de recours.

3. Lorsque cela est nécessaire à l'accomplissement de leurs missions au titre du présent règlement, les coordinateurs pour les services numériques sont également investis, à l'égard des fournisseurs de services intermédiaires relevant de la compétence de leur État membre, lorsque tous les autres pouvoirs prévus par le présent article pour parvenir à la cessation d'une infraction ont été épuisés, qu'il n'a pas été remédié à l'infraction ou que l'infraction se poursuit et qu'elle entraîne un préjudice grave ne pouvant pas être évité par l'exercice d'autres pouvoirs prévus par le droit de l'Union ou le droit national, du pouvoir de prendre les mesures suivantes:

a) exiger de l'organe de direction de ces fournisseurs, dans les meilleurs délais, qu'il examine la situation, adopte et soumette un plan d'action établissant les mesures nécessaires pour mettre fin à l'infraction, veille à ce que le fournisseur prenne ces mesures et fasse rapport sur les mesures prises;

b) lorsque le coordinateur pour les services numériques considère qu'un fournisseur de services intermédiaires n'a pas suffisamment respecté les exigences visées au point a), qu'il n'a pas été remédié à l'infraction ou que l'infraction se poursuit et qu'elle entraîne un préjudice grave, et que cette infraction constitue une infraction pénale impliquant une menace pour la vie ou la sécurité des personnes, demander à l'autorité judiciaire compétente de son État membre d'ordonner une restriction temporaire de l'accès des destinataires au service concerné par l'infraction ou, uniquement lorsque cela n'est pas techniquement réalisable, à l'interface en ligne du fournisseur de services intermédiaires sur laquelle se produit l'infraction.

Sauf lorsqu'il agit à la demande de la Commission au titre de l'article 82, préalablement à l'envoi de la demande visée au premier alinéa, point b), du présent paragraphe, le coordinateur pour les services numériques invite les parties intéressées à soumettre des observations écrites dans un délai de minimum deux semaines, en décrivant les mesures qu'il entend demander et en identifiant le ou les destinataires prévus. Le fournisseur de services intermédiaires, le ou les destinataires prévus et tout autre tiers démontrant un intérêt légitime ont le droit de participer à la procédure devant l'autorité judiciaire compétente. Toute mesure ordonnée est proportionnée à la nature, à la gravité, à la répétition et à la durée de l'infraction, et ne restreint pas indûment l'accès des destinataires du service concerné aux informations légales.

La restriction d'accès s'applique pour une durée de quatre semaines, sous réserve de la possibilité dont dispose l'autorité judiciaire compétente, dans son injonction, de permettre au coordinateur pour les services numériques de prolonger ce délai à raison de nouvelles périodes de même durée, le nombre maximal de prolongations étant fixé par cette autorité judiciaire. Le coordinateur pour les services numériques ne prolonge le délai que s'il considère, compte tenu des droits et des intérêts de toutes les parties affectées par cette limitation et de l'ensemble des circonstances pertinentes, y compris de toute information que le fournisseur de services intermédiaires, le ou les destinataires et tout autre tiers ayant démontré un intérêt légitime pourraient lui fournir, que les deux conditions suivantes sont remplies :

a) le fournisseur de services intermédiaires n'a pas pris les mesures nécessaires pour mettre fin à l'infraction;

b) la restriction temporaire ne restreint pas indûment l'accès des destinataires du service aux informations légales, compte tenu du nombre de destinataires affectés et de l'existence éventuelle de toute alternative appropriée et facilement accessible.

Lorsque le coordinateur pour les services numériques considère que les conditions énoncées au troisième alinéa, points a) et b), sont remplies, mais qu'il ne peut pas prolonger davantage la période visée au troisième alinéa, il soumet une nouvelle demande à l'autorité judiciaire compétente, conformément au premier alinéa, point b).

4. Les pouvoirs énumérés aux paragraphes 1, 2 et 3 sont sans préjudice de la section 3.

5. Les mesures prises par les coordinateurs pour les services numériques dans l'exercice de leurs pouvoirs énumérés aux paragraphes 1, 2 et 3 sont efficaces, proportionnées et dissuasives, compte tenu notamment de la nature, de la gravité, de la répétition et de la durée de l'infraction ou de l'infraction présumée à laquelle ces mesures se rapportent, ainsi que de la capacité économique, technique et opérationnelle du fournisseur de services intermédiaires concerné, le cas échéant.

6. Les États membres fixent des conditions et des procédures spécifiques pour l'exercice des pouvoirs visés aux paragraphes 1, 2 et 3 et veillent à ce que tout exercice de ces pouvoirs soit soumis à des mesures de sauvegarde appropriées établies dans le droit national applicable en conformité avec la Charte et les principes généraux du droit de l'Union. Plus particulièrement, ces mesures ne sont prises qu'en conformité avec le droit au respect de la vie privée et les droits de la défense, y compris les droits d'être entendu et d'avoir accès au dossier, et le droit à un recours juridictionnel effectif pour toutes les parties affectées.

Article 52 - Sanctions

1. Les États membres déterminent le régime des sanctions applicables aux infractions au présent règlement par les fournisseurs de services intermédiaires relevant de leur compétence et prennent toutes les mesures nécessaires pour assurer la mise en œuvre de ces sanctions conformément à l'article 51.

2. Les sanctions doivent être effectives, proportionnées et dissuasives. Les États membres informent la Commission du régime ainsi déterminé et des mesures ainsi prises, de même que, sans retard, de toute modification apportée ultérieurement à ce régime ou à ces mesures.

3. Les États membres veillent à ce que le montant maximal des amendes qui peuvent être imposées pour non-respect d'une obligation établie dans le présent règlement représente 6 % du chiffre d'affaires mondial annuel du fournisseur de services intermédiaires concerné réalisé au cours de l'exercice précédent. Les États membres veillent à ce que le montant maximal de l'amende qui peut être imposée pour la fourniture d'informations inexactes, incomplètes ou trompeuses, l'absence de réponse ou la non-rectification d'informations inexactes, incomplètes ou trompeuses et le manquement à l'obligation de se soumettre à une inspection représente 1 % des revenus ou du chiffre d'affaires mondial annuels du fournisseur de services intermédiaires concerné ou de la personne concernée de l'exercice précédent.

4. Les États membres veillent à ce que le montant maximal d'une astreinte représente 5 % des revenus ou du chiffre d'affaires mondial journaliers moyens du fournisseur de services intermédiaires concerné de l'exercice précédent, par jour, calculé à compter de la date spécifiée dans la décision concernée.

Article 53 - Droit d'introduire une plainte

Les destinataires du service, ainsi que tout organisme, organisation ou association ayant reçu mandat pour exercer les droits conférés par le présent règlement pour leur compte, ont le droit d'introduire une plainte à l'encontre de fournisseurs de services intermédiaires en invoquant une infraction au présent règlement auprès du coordinateur pour les services numériques de l'État membre dans lequel le destinataire du service est situé ou est établi. Le coordinateur pour les services numériques évalue la plainte et, le cas échéant, la transmet au coordinateur pour les services numériques de l'État membre d'établissement, accompagnée d'un avis lorsqu'il le juge approprié. Lorsque la plainte relève de la responsabilité d'une autre autorité compétente au sein de son État membre, le coordinateur pour les services numériques qui reçoit la plainte la transmet à cette autorité. Au cours de cette procédure, les deux parties ont le droit d'être entendues et de recevoir des informations appropriées sur l'état de la plainte, conformément au droit national.

Article 54 - Indemnisation

Les destinataires du service ont le droit de demander réparation aux fournisseurs de services intermédiaires, conformément au droit de l'Union et au droit national, pour les dommages ou pertes subis en raison d'une violation par lesdits fournisseurs des obligations qui leur incombent au titre du présent règlement.

Article 55 - Rapports d'activité

1. Les coordinateurs pour les services numériques établissent un rapport annuel relatif à leurs activités au titre du présent règlement, y compris le nombre de plaintes reçues en vertu de l'article 53 ainsi qu'un aperçu des suites qui leur ont été données. Les coordinateurs pour les services numériques mettent les rapports annuels à la disposition du public dans un format lisible par une machine, sous réserve des règles applicables en matière de confidentialité des informations en vertu de l'article 84, et les communiquent à la Commission et au comité.

2. Le rapport annuel comporte également les informations suivantes:

a) le nombre et l'objet des injonctions d'agir contre des contenus illicites et des injonctions de fournir des informations, émises conformément aux articles 9 et 10 par toute autorité judiciaire ou administrative nationale de l'État membre du coordinateur pour les services numériques concerné;

b) les suites données à ces injonctions, telles qu'elles ont été communiquées au coordinateur pour les services numériques conformément aux articles 9 et 10.

3. Lorsqu'un État membre a désigné plusieurs autorités compétentes conformément à l'article 49, il veille à ce que le coordinateur pour les services numériques élabore un rapport unique couvrant les activités de toutes les autorités compétentes et à ce que le coordinateur pour les services numériques reçoive toutes les informations pertinentes et tout le soutien nécessaire à cet effet de la part des autres autorités compétentes concernées.

SECTION 2

Compétences, enquête coordonnée et mécanismes de contrôle de la cohérence

Article 56 - Compétences

1. L'État membre dans lequel se situe l'établissement principal du fournisseur de services intermédiaires dispose de pouvoirs exclusifs pour surveiller et faire respecter le présent règlement, à l'exception des pouvoirs prévus aux paragraphes 2, 3 et 4.

2. La Commission dispose de pouvoirs exclusifs pour surveiller et faire respecter le chapitre III, section 5.

3. La Commission dispose de pouvoirs pour surveiller et faire respecter le présent règlement, autres que ceux fixés au chapitre III, section 5, à l'encontre des fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne.

4. Lorsque la Commission n'a pas engagé de procédure pour la même infraction, l'État membre dans lequel se situe l'établissement principal du fournisseur de très grandes plateformes en ligne ou de très grands moteurs de recherche en ligne dispose, à l'encontre desdits fournisseurs, de pouvoirs pour surveiller et faire respecter les obligations fixées dans le présent règlement, autres que ceux fixés au chapitre III, section 5.

5. Les États membres et la Commission surveillent et assurent le respect des dispositions du présent règlement en étroite coopération.

6. Lorsqu'un fournisseur de services intermédiaires ne dispose pas d'un établissement dans l'Union, l'État membre dans lequel son représentant légal réside ou est établi ou la Commission, selon le cas, dispose, conformément aux paragraphes 1 et 4 du présent article, de pouvoirs pour surveiller et faire respecter les obligations pertinentes fixées dans le présent règlement.

7. Lorsqu'un fournisseur de services intermédiaires ne désigne pas de représentant légal conformément à l'article 13, tous les États membres et, pour ce qui concerne les fournisseurs de très grandes plateformes en ligne ou de très grands moteurs de recherche en ligne, la Commission disposent de pouvoirs de surveillance et d'exécution conformément au présent article.

Lorsqu'un coordinateur des services numériques a l'intention d'exercer ses pouvoirs en vertu du présent paragraphe, il notifie son intention à tous les autres coordinateurs pour les services numériques ainsi qu'à la Commission et veille à ce que les garanties applicables prévues par la Charte soient respectées, notamment pour éviter que le même comportement ne soit sanctionné plus d'une fois pour une infraction aux obligations fixées par le présent règlement. Lorsque la Commission a l'intention d'exercer ses pouvoirs en vertu du présent paragraphe, elle notifie son intention à tous les autres coordinateurs pour les services numériques. À la suite de la notification visée au présent paragraphe, les autres États membres n'engagent pas de procédure pour la même infraction que celle dont il est question dans la notification.

Article 57 - Assistance mutuelle

1. Les coordinateurs pour les services numériques et la Commission coopèrent étroitement et se prêtent mutuellement assistance afin d'appliquer le présent règlement de manière cohérente et efficace. L'assistance mutuelle comprend, en particulier, l'échange d'informations conformément au présent article et l'obligation qui incombe au coordinateur pour les services numériques de l'État membre d'établissement d'informer tous les coordinateurs pour les services numériques des États membres de destination, le comité et la Commission de l'ouverture d'une enquête et de son intention de prendre une décision définitive, y compris son évaluation, à l'égard d'un fournisseur de services intermédiaires spécifique.

2. Aux fins d'une enquête, le coordinateur pour les services numériques de l'État membre d'établissement peut demander à d'autres coordinateurs pour les services numériques de fournir les informations spécifiques en leur possession concernant un fournisseur spécifique de services intermédiaires ou d'exercer leurs pouvoirs d'enquête visés à l'article 51, paragraphe 1, en ce qui concerne des informations spécifiques se trouvant dans leur État membre. Le cas échéant, le coordinateur pour les services numériques qui reçoit la demande peut associer d'autres autorités compétentes ou d'autres autorités publiques de l'État membre en question.

3. Le coordinateur pour les services numériques qui reçoit la demande conformément au paragraphe 2 y fait droit et informe le coordinateur pour les services numériques de l'État membre d'établissement des mesures prises, dans les meilleurs délais et au plus tard deux mois après la réception de la demande, sauf si:

a) la portée ou l'objet de la demande ne sont pas suffisamment précis, justifiés ou proportionnés au regard des objectifs de l'enquête; ou

b) ni le coordinateur pour les services numériques qui reçoit la demande ni aucune autre autorité compétente ou autorité publique de cet État membre n'est en possession des informations demandées ou ne peut accéder à celles-ci; ou

c) il n'est pas possible de faire droit à la demande sans violer le droit de l'Union ou le droit national.

Le coordinateur pour les services numériques qui reçoit la demande motive son refus en soumettant une réponse motivée, dans le délai fixé au premier alinéa.

Article 58 - Coopération transfrontière entre les coordinateurs pour les services numériques

1. Sauf dans le cas où la Commission a ouvert une enquête pour la même infraction alléguée, lorsqu'un coordinateur pour les services numériques d'un État membre de destination a des raisons de soupçonner que le fournisseur d'un service intermédiaire a enfreint le présent règlement d'une manière qui porte atteinte aux destinataires du service dans l'État membre dudit coordinateur pour les services numériques, il peut demander au coordinateur pour les services numériques de l'État membre d'établissement d'examiner la situation et de prendre les mesures d'enquête et d'exécution nécessaires pour assurer le respect du présent règlement.

2. Sauf dans le cas où la Commission a ouvert une enquête pour la même infraction alléguée, et à la demande d'au moins trois coordinateurs pour les services numériques d'États membres de destination, ayant des raisons de soupçonner qu'un fournisseur de services intermédiaires spécifique a enfreint le présent règlement d'une manière qui porte atteinte aux destinataires du service dans leur État membre, le comité peut demander au coordinateur pour les services numériques de l'État membre d'établissement d'examiner la situation et de prendre les mesures d'enquête et d'exécution nécessaires pour assurer le respect du présent règlement.

3. Toute demande formulée au titre du paragraphe 1 ou 2 est dûment motivée et indique au minimum :

a) le point de contact du fournisseur de services intermédiaires concerné, tel qu'il est prévu à l'article 11;

b) une description des faits pertinents, les dispositions concernées du présent règlement et les raisons pour lesquelles le coordinateur pour les services numériques à l'origine de la demande, ou le comité, soupçonne que le fournisseur a enfreint le présent règlement, y compris la description des effets négatifs de l'infraction alléguée;

c) toute autre information que le coordinateur pour les services numériques à l'origine de la demande, ou le comité, considère comme pertinente, y compris, le cas échéant, des informations recueillies de sa propre initiative ou des suggestions de mesures d'enquête ou d'exécution spécifiques à prendre, y compris des mesures provisoires.

4. Le coordinateur pour les services numériques de l'État membre d'établissement tient le plus grand compte de la demande formulée au titre du paragraphe 1 ou 2 du présent article. Lorsqu'il considère qu'il ne dispose pas de suffisamment d'informations pour agir sur la base de la demande et qu'il a des raisons de considérer que le coordinateur pour les services numériques à l'origine de la demande, ou le comité, pourrait fournir des informations complémentaires, le coordinateur pour les services numériques de l'État membre d'établissement peut soit demander ces informations conformément à l'article 57, soit lancer, en application de l'article 60, paragraphe 1, une enquête conjointe associant au moins le coordinateur pour les services numériques à l'origine de la demande. Le délai fixé au paragraphe 5 du présent article est suspendu jusqu'à l'obtention de ces informations complémentaires ou jusqu'à ce que l'invitation à participer à l'enquête conjointe ait été déclinée.

5. Dans les meilleurs délais et en tout état de cause dans un délai maximal de deux mois suivant la réception de la demande formulée au titre du paragraphe 1 ou 2, le coordinateur pour les services numériques de l'État membre d'établissement communique au coordinateur pour les services numériques à l'origine de la demande, et au comité, l'évaluation de l'infraction présumée, ainsi qu'une explication de toute mesure d'enquête ou d'exécution prise ou envisagée dans ce cadre afin d'assurer le respect du présent règlement.

Article 59 - Saisine de la Commission

1. En l'absence de communication dans le délai fixé à l'article 58, paragraphe 5, en cas de désaccord de la part du comité avec l'évaluation ou les mesures prises ou envisagées au titre de l'article 58, paragraphe 5, ou dans les cas visés à l'article 60, paragraphe 3, le comité peut saisir la Commission de la question, en fournissant toutes les informations pertinentes. Ces informations comprennent au moins la demande ou la recommandation envoyée au coordinateur pour les services numériques de l'État membre d'établissement, l'évaluation réalisée par ce coordinateur pour les services numériques, les raisons du désaccord ainsi que toute information complémentaire justifiant la saisine.

2. La Commission examine la question dans un délai de deux mois suivant la transmission de la question en vertu du paragraphe 1, après avoir consulté le coordinateur pour les services numériques de l'État membre d'établissement.

3. Lorsque, en vertu du paragraphe 2 du présent article, la Commission considère que l'évaluation ou les mesures d'enquête ou d'exécution prises ou envisagées au titre de l'article 58, paragraphe 5, sont insuffisantes pour garantir l'exécution effective du présent règlement ou sont, d'une autre façon, incompatibles avec le présent règlement, elle fait part de son point de vue au coordinateur pour les services numériques de l'État membre d'établissement ainsi qu'au comité, et demande au coordinateur pour les services numériques de l'État membre d'établissement de réexaminer la question.

Le coordinateur pour les services numériques de l'État membre d'établissement prend les mesures d'enquête ou d'exécution nécessaires en vue d'assurer le respect du présent règlement, en tenant le plus grand compte du point de vue et de la demande de réexamen de la Commission. Le coordinateur pour les services numériques de l'État membre d'établissement informe la Commission et le coordinateur pour les services numériques à l'origine de la demande ou le comité qui est intervenu au titre de l'article 58, paragraphe 1 ou 2, des mesures prises dans les deux mois à compter de cette demande de réexamen.

Article 60- Enquêtes conjointes

1. Le coordinateur pour les services numériques de l'État membre d'établissement peut lancer et diriger des enquêtes conjointes avec la participation d'un ou de plusieurs coordinateurs pour les services numériques concernés:

a) de sa propre initiative, en ce qui concerne une infraction alléguée au présent règlement commise par un fournisseur de services intermédiaires donné dans plusieurs États membres; ou

b) sur recommandation du comité, à la demande d'au moins trois coordinateurs pour les services numériques alléguant, sur la base d'une suspicion raisonnable, l'existence d'une infraction commise par un fournisseur de services intermédiaires donné, portant atteinte aux destinataires du service dans leur État membre.

2. Tout coordinateur pour les services numériques qui démontre qu'il a un intérêt légitime à participer à une enquête conjointe conformément au paragraphe 1 peut demander à le faire. L'enquête conjointe est menée à terme dans un délai de trois mois à compter du moment où elle a été lancée, sauf si les participants en conviennent autrement.

Le coordinateur pour les services numériques de l'État membre d'établissement communique à tous les coordinateurs pour les services numériques, à la Commission et au comité sa position préliminaire sur l'infraction alléguée au plus tard un mois après la fin du délai visé au premier alinéa. La position préliminaire tient compte du point de vue de tous les autres coordinateurs pour les services numériques participant à l'enquête conjointe. Le cas échéant, cette position préliminaire expose également les mesures d'exécution envisagées.

3. Le comité peut saisir la Commission conformément à l'article 59, lorsque:

a) le coordinateur pour les services numériques de l'État membre d'établissement n'a pas communiqué sa position préliminaire dans le délai fixé au paragraphe 2;

b) le comité exprime un désaccord important avec la position préliminaire communiquée par le coordinateur pour les services numériques de l'État membre d'établissement; ou

c) le coordinateur pour les services numériques de l'État membre d'établissement n'a pas lancé l'enquête conjointe promptement à la suite de la recommandation du comité visée au paragraphe 1, point b).

4. Lorsqu'ils procèdent à une enquête conjointe, les coordinateurs pour les services numériques participants coopèrent de bonne foi, en tenant compte, le cas échéant, des indications du coordinateur pour les services numériques de l'État membre d'établissement et de la recommandation du comité. Les coordinateurs pour les services numériques des États membres de destination participant à l'enquête conjointe sont habilités, à la demande du coordinateur pour les services numériques de l'État membre d'établissement ou après l'avoir consulté, à exercer leurs pouvoirs d'enquête visés à l'article 51, paragraphe 1, à l'égard des fournisseurs de services intermédiaires concernés par l'infraction alléguée, en ce qui concerne les informations et les locaux situés sur leur territoire.

SECTION 3

Comité européen des services numériques

Article 61- Comité européen des services numériques

1. Un groupe consultatif indépendant de coordinateurs pour les services numériques, dénommé "comité européen des services numériques" (ci-après dénommé "comité") est établi pour assurer la surveillance des fournisseurs de services intermédiaires.

2. Le comité conseille les coordinateurs pour les services numériques et la Commission conformément au présent règlement pour atteindre les objectifs suivants:

a) contribuer à l'application cohérente du présent règlement et à la coopération efficace des coordinateurs pour les services numériques et de la Commission en ce qui concerne les matières relevant du présent règlement;

b) coordonner les lignes directrices et les analyses de la Commission et des coordinateurs pour les services numériques et d'autres autorités compétentes sur les questions émergentes dans l'ensemble du marché intérieur en ce qui concerne les matières relevant du présent règlement, et y contribuer;

c) assister les coordinateurs pour les services numériques et la Commission dans la surveillance des très grandes plateformes en ligne.

Article 62 - Structure du comité

1. Le comité se compose des coordinateurs pour les services numériques qui sont représentés par de hauts fonctionnaires. Le fait qu'un ou plusieurs États membres ne désignent pas de coordinateur pour les services numériques ne fait pas obstacle à ce que le comité exécute ses tâches au titre du présent règlement. Lorsque le droit national le prévoit, d'autres autorités compétentes investies de responsabilités opérationnelles spécifiques en vue de l'application et de l'exécution du présent règlement peuvent participer au comité aux côtés du coordinateur pour les services numériques. D'autres autorités nationales peuvent être invitées aux réunions, lorsque les questions examinées relèvent de leurs compétences.

2. Le comité est présidé par la Commission. La Commission convoque les réunions et prépare l'ordre du jour conformément aux missions du comité au titre du présent règlement et à son règlement intérieur. Lorsque le comité est saisi d'une demande d'adopter une recommandation en vertu du présent règlement, il met immédiatement cette demande à la disposition des autres coordinateurs pour les services numériques via le système de partage d'informations prévu à l'article 85.

3. Chaque État membre dispose d'une voix. La Commission n'a pas de droit de vote.

Le comité adopte ses décisions à la majorité simple. Lorsqu'il adopte une recommandation destinée à la Commission ainsi que le prévoit l'article 36, paragraphe 1, premier alinéa, le comité vote dans les 48 heures suivant la demande du président du comité.

4. La Commission apporte un appui administratif et analytique aux activités du comité au titre du présent règlement.

5. Le comité peut inviter des experts et des observateurs à participer à ses réunions, et peut coopérer avec d'autres organes, organismes et groupes consultatifs de l'Union, ainsi qu'avec des experts externes, le cas échéant. Le comité rend publics les résultats de cette coopération.

6. Le comité peut consulter les parties intéressées et rend publics les résultats de telles consultations.

7. Le comité adopte son règlement intérieur une fois celui-ci approuvé par la Commission.

Article 63 - Missions du comité

1. Lorsque cela est nécessaire pour réaliser les objectifs énoncés à l'article 61, paragraphe 2, le comité:

a) soutient la coordination d'enquêtes conjointes;

b) soutient les autorités compétentes dans l'analyse des rapports et résultats des audits réalisés auprès des très grandes plateformes en ligne ou des très grands moteurs de recherche en ligne dont le présent règlement prévoit la transmission;

c) émet des avis, des recommandations ou des conseils destinés aux coordinateurs pour les services numériques conformément au présent règlement, en tenant compte notamment de la liberté des fournisseurs de services intermédiaires de fournir des services;

d) conseille la Commission en ce qui concerne les mesures visées à l'article 66 et adopte des avis concernant les très grandes plateformes en ligne ou les très grands moteurs de recherche en ligne conformément au présent règlement;

e) soutient et encourage l'élaboration et la mise en œuvre de normes européennes, lignes directrices, rapports, modèles et codes de conduite, en collaboration avec les parties prenantes pertinentes, comme le prévoit le présent règlement, y compris en émettant des avis ou des recommandations sur les questions liées à l'article 44, ainsi que l'identification des questions émergentes, en ce qui concerne les matières relevant du présent règlement.

2. Les coordinateurs pour les services numériques et, selon le cas, d'autres autorités compétentes qui ne suivent pas les avis, demandes ou recommandations adoptés par le comité qui leur ont été adressés motivent ce choix, notamment en donnant une explication concernant les enquêtes, actions et mesures qu'ils ont mises en œuvre dans les rapports qu'ils établissent conformément au présent règlement ou lors de l'adoption des décisions pertinentes, le cas échéant.

SECTION 4

Surveillance, enquêtes, exécution et contrôle concernant les fournisseurs de très grandes plateformes en ligne ou de très grands moteurs de recherche en ligne

Article 64 - Développement de l'expertise et des capacités

1. La Commission, en coopération avec les coordinateurs pour les services numériques et le comité, développe l'expertise et les capacités de l'Union, y compris, le cas échéant, en détachant du personnel des États membres.

2. En outre, la Commission, en coopération avec les coordinateurs pour les services numériques et le comité, coordonne l'évaluation des questions systémiques et émergentes relatives aux très grandes plateformes en ligne ou aux très grands moteurs de recherche en

ligne qui se posent dans l'ensemble de l'Union en ce qui concerne les matières relevant du présent règlement.

3. La Commission peut demander aux coordinateurs pour les services numériques, au comité et à d'autres organes ou organismes de l'Union disposant de l'expertise pertinente de soutenir l'évaluation des questions systémiques et émergentes qui se posent dans l'ensemble de l'Union au titre du présent règlement.

4. Les États membres coopèrent avec la Commission, en particulier, par l'intermédiaire de leurs coordinateurs pour les services numériques respectifs et d'autres autorités compétentes, le cas échéant, y compris en mettant à disposition leur expertise et leurs capacités.

Article 65 - Exécution des obligations des fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne

1. À des fins d'enquête sur le respect, par les fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne, des obligations fixées par le présent règlement, la Commission peut exercer les pouvoirs d'enquête prévus dans la présente section avant même d'engager la procédure prévue à l'article 66, paragraphe 2. Elle peut exercer ces pouvoirs de sa propre initiative ou à la suite d'une demande formulée en vertu du paragraphe 2 du présent article.

2. Lorsqu'un coordinateur pour les services numériques a des raisons de soupçonner qu'un fournisseur d'une très grande plateforme en ligne ou d'un très grand moteur de recherche en ligne a enfreint les dispositions du chapitre III, section 5, ou a systématiquement enfreint l'une des dispositions du présent règlement d'une manière qui affecte gravement les destinataires du service dans son État membre, il peut envoyer à la Commission, via le système de partage d'informations prévu à l'article 85, une demande d'examen de la question.

3. Toute demande formulée en vertu du paragraphe 2 est dûment motivée et indique au minimum:

a) le point de contact du fournisseur de la très grande plateforme en ligne ou du très grand moteur de recherche en ligne concerné, comme prévu à l'article 11;

b) une description des faits pertinents, les dispositions du présent règlement concernées et les raisons pour lesquelles le coordinateur pour les services numériques à l'origine de la demande soupçonne que le fournisseur de la très grande plateforme en ligne ou du très grand moteur de recherche en ligne concerné a enfreint le présent règlement, avec une description des faits montrant que l'infraction présumée est de nature systémique;

c) toute autre information que le coordinateur pour les services numériques à l'origine de la demande juge pertinente, y compris, le cas échéant, les informations recueillies de sa propre initiative.

Article 66 - Procédures engagées par la Commission et coopération à l'enquête

1. La Commission peut engager une procédure en vue de l'éventuelle adoption de décisions au titre des articles 73 et 74 à l'égard de la conduite en cause du fournisseur de la très grande

plateforme en ligne ou du très grand moteur de recherche en ligne que la Commission soupçonne d'avoir enfreint l'une des dispositions du présent règlement.

2. Lorsque la Commission décide d'engager une procédure en vertu du paragraphe 1 du présent article, elle en informe tous les coordinateurs pour les services numériques et le comité via le système de partage d'informations visé à l'article 85, ainsi que le fournisseur de la très grande plateforme en ligne ou du très grand moteur de recherche en ligne concerné.

Les coordinateurs pour les services numériques transmettent à la Commission, dans les meilleurs délais après avoir été informés qu'une procédure a été engagée, toutes les informations qu'ils détiennent au sujet de l'infraction en cause.

L'engagement d'une procédure par la Commission en vertu du paragraphe 1 du présent article relève le coordinateur pour les services numériques, ou toute autorité compétente selon le cas, de ses pouvoirs de surveillance et d'exécution prévus dans le présent règlement conformément à l'article 56, paragraphe 4.

3. Dans l'exercice des pouvoirs d'enquête que lui confère le présent règlement, la Commission peut demander l'aide individuelle ou conjointe des coordinateurs pour les services numériques concernés par l'infraction présumée, notamment du coordinateur pour les services numériques de l'État membre d'établissement. Les coordinateurs pour les services numériques qui ont reçu une telle demande, ainsi que toute autre autorité compétente à laquelle le coordinateur pour les services numériques fait appel, coopèrent de bonne foi et en temps utile avec la Commission et sont habilités à exercer leurs pouvoirs d'enquête visés à l'article 51, paragraphe 1, à l'égard de la très grande plateforme en ligne ou du très grand moteur de recherche en ligne en question, pour ce qui est des informations, des personnes et des locaux situés sur le territoire de leur État membre et conformément à la demande.

4. La Commission fournit au coordinateur pour les services numériques de l'État membre d'établissement et au comité toutes les informations pertinentes sur l'exercice des pouvoirs visés aux articles 67 à 72 et ses conclusions préliminaires conformément à l'article 79, paragraphe 1. Le comité fait part à la Commission de son point de vue sur les conclusions préliminaires dans le délai fixé en vertu de l'article 79, paragraphe 2. La Commission tient le plus grand compte du point de vue du comité dans sa décision.

Article 67 - Demandes d'informations

1. Pour l'accomplissement des tâches qui lui sont assignées par la présente section, la Commission peut, par simple demande ou par voie de décision, requérir du fournisseur de la très grande plateforme en ligne ou du très grand moteur de recherche en ligne concerné, ainsi que de toute autre personne physique ou morale agissant pour les besoins de leur activité commerciale, industrielle, artisanale ou libérale qui est raisonnablement susceptible d'avoir connaissance d'informations relatives à l'infraction présumée, y compris des organisations qui réalisent les audits visés à l'article 37 et à l'article 75, paragraphe 2, qu'ils fournissent ces informations dans un délai raisonnable.

2. Lorsqu'elle envoie une simple demande d'informations au fournisseur de la très grande plateforme en ligne ou du très grand moteur de recherche en ligne concerné ou à une autre personne visée au paragraphe 1 du présent article, la Commission indique la base juridique et le but de la demande, précise les informations demandées et fixe le délai dans lequel elles

doivent être fournies. Elle mentionne également les amendes prévues à l'article 74 au cas où une information inexacte, incomplète ou trompeuse serait fournie.

3. Lorsque la Commission requiert, par voie de décision, du fournisseur de la très grande plateforme en ligne ou du très grand moteur de recherche en ligne concerné ou d'une autre personne visée au paragraphe 1 du présent article, qu'ils fournissent des informations, elle indique la base juridique et le but de la demande, précise les informations demandées et fixe le délai dans lequel elles doivent être fournies. Elle mentionne également les amendes prévues à l'article 74 et mentionne ou inflige les astreintes prévues à l'article 76. Elle mentionne également le droit de faire réexaminer la décision par la Cour de justice de l'Union européenne.

4. Les fournisseurs de la très grande plateforme en ligne ou du très grand moteur de recherche en ligne concernés ou une autre personne visée au paragraphe 1 ou leurs représentants et, dans le cas de personnes morales, de sociétés ou d'associations n'ayant pas la personnalité juridique, les personnes mandatées pour les représenter selon la loi ou les statuts, sont tenus de fournir les informations demandées au nom du fournisseur de la très grande plateforme en ligne ou du très grand moteur de recherche en ligne concerné ou d'une autre personne visée au paragraphe 1. Les avocats dûment mandatés peuvent fournir les informations demandées au nom de leurs mandants. Ces derniers voient leur responsabilité pleinement engagée si les informations fournies s'avèrent incomplètes, inexactes ou trompeuses.

5. À la demande de la Commission, les coordinateurs pour les services numériques et autres autorités compétentes fournissent à la Commission toutes les informations nécessaires à l'accomplissement des tâches qui lui sont assignées par la présente section.

6. La Commission, sans retard injustifié après avoir envoyé la simple demande ou la décision visée au paragraphe 1 du présent article, en envoie une copie aux coordinateurs pour les services numériques, par l'intermédiaire du système de partage d'informations visé à l'article 85.

Article 68 - Pouvoir de mener des entretiens et de recueillir des déclarations

1. Pour l'accomplissement des tâches qui lui sont assignées par la présente section, la Commission peut interroger toute personne physique ou morale qui consent à être interrogée aux fins de la collecte d'informations relatives à l'objet d'une enquête, en lien avec l'infraction présumée. La Commission est habilitée à enregistrer ces entretiens par des moyens techniques appropriés.

2. Si l'entretien visé au paragraphe 1 se déroule dans d'autres locaux que ceux de la Commission, celle-ci en informe le coordinateur pour les services numériques de l'État membre sur le territoire duquel l'entretien a lieu. À la demande dudit coordinateur pour les services numériques, ses fonctionnaires peuvent assister les fonctionnaires et les autres personnes les accompagnant mandatés par la Commission pour mener l'entretien.

Article 69 - Pouvoir d'effectuer des inspections

1. Pour l'accomplissement des tâches qui lui sont assignées par la présente section, la Commission peut effectuer toutes les inspections nécessaires dans les locaux du fournisseur

de la très grande plateforme en ligne ou du très grand moteur de recherche en ligne concerné ou d'une autre personne visée à l'article 67, paragraphe 1.

2. Les fonctionnaires et les autres personnes les accompagnant mandatés par la Commission pour effectuer une inspection sont investis des pouvoirs suivants:

a) pénétrer dans tous les locaux, terrains et moyens de transport du fournisseur de la très grande plateforme en ligne ou du très grand moteur de recherche en ligne concerné ou de l'autre personne concernée;

b) examiner les livres et autres registres relatifs à la fourniture du service concerné, quel que soit le support sur lequel ils sont stockés;

c) prendre ou obtenir sous quelque forme que ce soit une copie ou un extrait des livres ou autres registres;

d) exiger du fournisseur de la très grande plateforme en ligne ou du très grand moteur de recherche en ligne ou de l'autre personne concernée qu'il donne accès à son organisation, à son fonctionnement, à son système informatique, à ses algorithmes, à son traitement des données et à ses pratiques commerciales, qu'il fournisse des explications à ce sujet et qu'il enregistre ou documente les explications données;

e) sceller tout local utilisé pour les besoins de l'activité commerciale, industrielle, artisanale ou libérale du fournisseur de la très grande plateforme en ligne ou du très grand moteur de recherche en ligne ou de l'autre personne concernée, ainsi que les livres ou autres registres, pendant la période d'inspection et dans la mesure nécessaires à l'inspection;

f) demander à tout représentant ou membre du personnel du fournisseur de la très grande plateforme en ligne ou du très grand moteur de recherche en ligne ou de l'autre personne concernée, des explications sur des faits ou des documents en rapport avec l'objet et le but de l'inspection et enregistrer les réponses;

g) adresser des questions à tout représentant ou membre du personnel en rapport avec l'objet et le but de l'inspection et enregistrer les réponses.

3. Les inspections peuvent être effectuées avec le concours d'auditeurs ou d'experts nommés par la Commission en vertu de l'article 72, paragraphe 2, et du coordinateur pour les services numériques ou des autorités nationales compétentes de l'État membre sur le territoire duquel l'inspection est menée.

4. Lorsque les livres ou autres registres liés à la fourniture du service concerné dont la production est requise sont produits de manière incomplète ou lorsque les réponses aux questions posées en vertu du paragraphe 2 du présent article sont inexactes, incomplètes ou trompeuses, les fonctionnaires et les autres personnes les accompagnant mandatés par la Commission pour effectuer une inspection exercent leurs pouvoirs sur présentation d'une autorisation écrite précisant l'objet et le but de l'inspection ainsi que les sanctions prévues aux articles 74 et 76. En temps utile avant l'inspection, la Commission informe de l'inspection prévue le coordinateur pour les services numériques de l'État membre sur le territoire duquel l'inspection doit être effectuée.

5. Au cours des inspections, les fonctionnaires et les autres personnes les accompagnant mandatés par la Commission, les auditeurs et les experts nommés par la Commission, le coordinateur pour les services numériques ou les autres autorités compétentes de l'État membre sur le territoire duquel l'inspection est effectuée peuvent exiger du fournisseur de la très grande plateforme en ligne ou du très grand moteur de recherche en ligne, ou de l'autre personne concernée, qu'il fournisse des explications sur son organisation, son fonctionnement, son système informatique, ses algorithmes, son traitement des données et ses pratiques commerciales, et peuvent adresser des questions à son personnel clé.

6. Le fournisseur de la très grande plateforme en ligne ou du très grand moteur de recherche en ligne ou l'autre personne physique ou morale concernée est tenu de se soumettre aux inspections que la Commission a ordonnées par voie de décision. La décision indique l'objet et le but de l'inspection, fixe la date à laquelle elle commence et mentionne les sanctions prévues aux articles 74 et 76, ainsi que le droit de faire réexaminer la décision par la Cour de justice de l'Union européenne. La Commission consulte le coordinateur pour les services numériques de l'État membre sur le territoire duquel l'inspection doit être effectuée avant de prendre cette décision.

7. Les agents du coordinateur pour les services numériques de l'État membre sur le territoire duquel l'inspection doit être effectuée et les autres personnes mandatées ou nommées par ledit coordinateur prêtent activement assistance, à la demande dudit coordinateur pour les services numériques ou de la Commission, aux fonctionnaires et aux autres personnes les accompagnant mandatés par la Commission dans le cadre de l'inspection. Ils disposent à cette fin des pouvoirs énumérés au paragraphe 2.

8. Lorsque les fonctionnaires et les autres personnes les accompagnant mandatés par la Commission constatent que le fournisseur de la très grande plateforme en ligne ou du très grand moteur de recherche en ligne, ou l'autre personne concernée, s'oppose à une inspection ordonnée en vertu du présent article, l'État membre sur le territoire duquel l'inspection doit être effectuée leur accorde, sur demande de ces fonctionnaires ou des autres personnes les accompagnant et conformément au droit national de l'État membre, l'assistance nécessaire, y compris, le cas échéant conformément audit droit national, sous la forme de mesures coercitives prises par une autorité répressive compétente, pour leur permettre d'effectuer l'inspection.

9. Si l'assistance prévue au paragraphe 8 requiert l'autorisation d'une autorité judiciaire nationale conformément au droit national de l'État membre concerné, cette autorisation est demandée par le coordinateur pour les services numériques de cet État membre à la demande des fonctionnaires et des autres personnes les accompagnant mandatés par la Commission. Cette autorisation peut également être demandée à titre préventif.

10. Lorsqu'une autorisation visée au paragraphe 9 est demandée, l'autorité judiciaire nationale saisie vérifie que la décision de la Commission ordonnant l'inspection est authentique et que les mesures coercitives envisagées ne sont ni arbitraires ni excessives eu égard à l'objet de l'inspection. Lorsqu'elle procède à cette vérification, l'autorité judiciaire nationale peut demander à la Commission, directement ou par l'intermédiaire des coordinateurs pour les services numériques de l'État membre concerné, des explications détaillées notamment sur les motifs permettant à la Commission de suspecter l'existence d'une infraction au présent règlement, ainsi que sur la gravité de l'infraction suspectée et la

nature de l'implication du fournisseur de la très grande plateforme en ligne ou du très grand moteur de recherche en ligne ou de l'autre personne concernée. Cependant, l'autorité judiciaire nationale ne peut ni remettre en cause la nécessité de l'inspection ni exiger la communication d'informations figurant dans le dossier de la Commission. Le contrôle de la légalité de la décision de la Commission est réservé à la Cour de justice de l'Union européenne.

Article 70 - Mesures provisoires

1. Dans le contexte des procédures susceptibles de mener à l'adoption d'une décision constatant un manquement en application de l'article 73, paragraphe 1, en cas d'urgence justifiée par le fait qu'un préjudice grave risque d'être causé aux destinataires du service, la Commission peut, par voie de décision, ordonner des mesures provisoires à l'encontre du fournisseur de la très grande plateforme en ligne ou du très grand moteur de recherche en ligne concerné sur la base d'un constat prima facie d'infraction.

2. Une décision prise en vertu du paragraphe 1 est applicable pour une durée déterminée et est renouvelable dans la mesure où cela est nécessaire et opportun.

Article 71- Engagements

1. Si, au cours d'une procédure au titre de la présente section, le fournisseur de la très grande plateforme en ligne ou du très grand moteur de recherche en ligne concerné propose des engagements afin de garantir le respect des dispositions pertinentes du présent règlement, la Commission peut, par voie de décision, rendre ces engagements contraignants pour le fournisseur de la très grande plateforme en ligne ou du très grand moteur de recherche en ligne concerné et déclarer qu'il n'y a plus lieu d'agir.

2. La Commission peut rouvrir la procédure, sur demande ou de sa propre initiative:

   a) si l'un des faits sur lesquels la décision repose subit un changement important;

   b) si le fournisseur concerné de la très grande plateforme en ligne ou du très grand moteur de recherche en ligne contrevient à ses engagements; ou

   c) si la décision reposait sur des informations incomplètes, inexactes ou trompeuses fournies par le fournisseur de la très grande plateforme en ligne ou du très grand moteur de recherche en ligne concerné ou une autre personne visée à l'article 67, paragraphe 1.

3. Si la Commission estime que les engagements proposés par le fournisseur de la très grande plateforme en ligne ou du très grand moteur de recherche en ligne concerné ne permettent pas de garantir le respect effectif des dispositions pertinentes du présent règlement, elle rejette ces engagements dans une décision motivée lors de la clôture de la procédure.

Article 72 - Mesures de contrôle

1. Pour l'accomplissement des tâches qui lui sont assignées par la présente section, la Commission peut prendre les mesures nécessaires pour contrôler la mise en œuvre et le respect effectifs du présent règlement par les fournisseurs des très grandes plateformes en

ligne ou des très grands moteurs de recherche en ligne concernés. La Commission peut leur ordonner de donner accès à leurs bases de données et algorithmes, ainsi que de fournir des explications à cet égard. Ces mesures peuvent notamment imposer au fournisseur de la très grande plateforme en ligne ou du très grand moteur de recherche en ligne l'obligation de conserver tous les documents jugés nécessaires pour évaluer la mise en œuvre et le respect des obligations prévues par le présent règlement.

2. Les mesures visées au paragraphe 1 peuvent comprendre la nomination d'experts et d'auditeurs externes indépendants, ainsi que d'experts et d'auditeurs des autorités nationales compétentes avec l'accord de l'autorité concernée, pour aider la Commission à contrôler la mise en œuvre et le respect effectifs des dispositions pertinentes du présent règlement et lui apporter une expertise et des connaissances spécifiques.

Article 73 - Non-respect

1. La Commission adopte une décision constatant un manquement lorsqu'elle constate que le fournisseur de la très grande plateforme en ligne ou du très grand moteur de recherche en ligne concerné ne respecte pas un ou plusieurs des éléments suivants:

a) les dispositions pertinentes du présent règlement;

b) les mesures provisoires ordonnées en vertu de l'article 70;

c) les engagements rendus contraignants en vertu de l'article 71.

2. Avant d'adopter la décision visée au paragraphe 1, la Commission fait part de ses constatations préliminaires au fournisseur de la très grande plateforme en ligne ou du très grand moteur de recherche en ligne concerné. Dans ses constatations préliminaires, la Commission explique les mesures qu'elle envisage de prendre, ou que le fournisseur concerné de la très grande plateforme en ligne ou du très grand moteur de recherche en ligne devrait prendre, selon elle, afin de donner suite de manière effective aux constatations préliminaires.

3. Dans la décision adoptée en vertu du paragraphe 1, la Commission ordonne au fournisseur de la très grande plateforme en ligne ou du très grand moteur de recherche en ligne concerné de prendre les mesures nécessaires pour assurer le respect de ladite décision dans un délai approprié qui y est précisé et de fournir des informations relatives aux mesures que ledit fournisseur entend adopter pour respecter la décision.

4. Le fournisseur de la très grande plateforme en ligne ou du très grand moteur de recherche en ligne concerné fournit à la Commission la description des mesures qu'il a prises pour garantir le respect de la décision adoptée en vertu du paragraphe 1 lors de leur mise en œuvre.

5. Lorsque la Commission constate que les conditions énoncées au paragraphe 1 ne sont pas réunies, elle clôt l'enquête par voie de décision. La décision est applicable avec effet immédiat.

Article 74 - Amendes

1. Dans la décision visée à l'article 73, la Commission peut infliger au fournisseur de la très grande plateforme en ligne ou du très grand moteur de recherche en ligne concerné des

amendes jusqu'à concurrence de 6 % du chiffre d'affaires mondial annuel réalisé au cours de l'exercice précédent lorsqu'elle constate que ledit fournisseur, de propos délibéré ou par négligence:

a) enfreint les dispositions pertinentes du présent règlement;

b) ne respecte pas une décision ordonnant des mesures provisoires en application de l'article 70; ou

c) ne respecte pas un engagement rendu contraignant par voie de décision en vertu de l'article 71.

2. La Commission peut adopter une décision visant à infliger au fournisseur de la très grande plateforme en ligne ou du très grand moteur de recherche concerné, ou à une autre personne physique ou morale visée à l'article 67, paragraphe 1, des amendes jusqu'à concurrence de 1 % des revenus ou du chiffre d'affaires mondial annuels de l'exercice précédent lorsque, de propos délibéré ou par négligence, ils:

a) fournissent des informations inexactes, incomplètes ou trompeuses en réponse à une simple demande ou à une demande par voie de décision, conformément à l'article 67;

b) omettent de répondre à la demande d'informations par voie de décision dans le délai fixé;

c) omettent de rectifier, dans le délai fixé par la Commission, les informations inexactes, incomplètes ou trompeuses fournies par un membre du personnel, ou omettent ou refusent de fournir des informations complètes;

d) refusent de se soumettre à une inspection décidée en vertu de l'article 69;

e) ne respectent pas les mesures adoptées par la Commission en vertu de l'article 72; ou

f) ne respectent pas les conditions d'accès au dossier de la Commission prévues à l'article 79, paragraphe 4.

3. Avant d'adopter la décision au titre du paragraphe 2 du présent article, la Commission fait part de ses constatations préliminaires au fournisseur de la très grande plateforme en ligne ou du très grand moteur de recherche en ligne concerné, ou à une autre personne visée à l'article 67, paragraphe 1.

4. Pour déterminer le montant de l'amende, la Commission prend en considération la nature, la gravité, la durée et la répétition de l'infraction ainsi que, pour les amendes infligées au titre du paragraphe 2, le retard causé à la procédure.

Article 75 - Surveillance renforcée des voies de recours pour remédier aux violations des obligations prévues au chapitre III, section 5

1. Lorsqu'elle adopte une décision en vertu de l'article 73 concernant la violation par un fournisseur d'une très grande plateforme en ligne ou d'un très grand moteur de recherche en ligne de l'une des dispositions du chapitre III, section 5, la Commission fait usage du système

de surveillance renforcée prévu au présent article. Ce faisant, elle tient le plus grand compte des avis du comité au titre du présent article.

2. Dans la décision visée à l'article 73, la Commission demande au fournisseur d'une très grande plateforme en ligne ou d'un très grand moteur de recherche en ligne concerné d'élaborer et de communiquer, dans un délai raisonnable précisé dans la décision, aux coordinateurs pour les services numériques, à la Commission et au comité, un plan d'action exposant les mesures nécessaires pour mettre fin à l'infraction ou y remédier. Ces mesures comprennent un engagement à réaliser un audit indépendant conformément à l'article 37, paragraphes 3 et 4, sur la mise en œuvre des autres mesures, et précisent l'identité des auditeurs ainsi que la méthodologie, le calendrier et le suivi de l'audit. Les mesures peuvent également comprendre, le cas échéant, l'engagement de participer à un code de conduite pertinent tel qu'il est prévu à l'article 45.

3. Dans un délai d'un mois suivant la réception du plan d'action, le comité communique son avis sur celui-ci à la Commission. Dans un délai d'un mois suivant la réception de cet avis, la Commission décide si les mesures prévues dans le plan d'action sont suffisantes pour mettre fin à l'infraction ou y remédier et fixe un délai raisonnable pour sa mise en œuvre. L'engagement éventuel d'adhérer aux codes de conduite pertinents est pris en compte dans cette décision. La Commission contrôle ensuite la mise en œuvre du plan d'action. À cette fin, le fournisseur d'une très grande plateforme en ligne ou d'un très grand moteur de recherche en ligne concerné communique le rapport d'audit à la Commission sans retard injustifié dès qu'il est disponible et tient la Commission informée des mesures prises pour la mise en œuvre du plan d'action. La Commission peut, lorsque cela est nécessaire aux fins d'un tel contrôle, exiger du fournisseur d'une très grande plateforme en ligne ou d'un très grand moteur de recherche en ligne concerné qu'il fournisse des informations supplémentaires dans un délai raisonnable fixé par la Commission.

La Commission tient le comité et les coordinateurs pour les services numériques informés de la mise en œuvre du plan d'action et de son suivi.

4. La Commission peut prendre les mesures nécessaires conformément au présent règlement, et notamment à l'article 76, paragraphe 1, point e), et à l'article 82, paragraphe 1, lorsque:

a) le fournisseur concerné de la très grande plateforme en ligne ou du très grand moteur de recherche en ligne ne fournit pas de plan d'action, le rapport d'audit, les mises à jour nécessaires ou toute information supplémentaire requise, dans le délai applicable;

b) la Commission rejette le plan d'action proposé, car elle estime que les mesures qui y sont énoncées sont insuffisantes pour mettre fin à l'infraction ou y remédier; ou

c) la Commission considère, sur la base du rapport d'audit, des mises à jour ou des informations supplémentaires fournies ou de toute autre information pertinente dont elle dispose, que la mise en œuvre du plan d'action est insuffisante pour mettre fin à l'infraction ou y remédier.

Article 76- Astreintes

1. La Commission peut adopter une décision visant à infliger au fournisseur de la très grande plateforme en ligne ou du très grand moteur de recherche concerné ou à une autre personne

visée à l'article 67, paragraphe 1, selon le cas, des astreintes jusqu'à concurrence de 5 % des revenus ou du chiffre d'affaires mondial journaliers moyens de l'exercice précédent par jour, calculées à compter de la date qu'elle fixe dans sa décision, pour les contraindre:

a) à fournir des informations exactes et complètes en réponse à une demande d'informations par voie de décision en application de l'article 67;

b) à se soumettre à une inspection ordonnée par voie de décision prise en vertu de l'article 69;

c) à respecter une décision ordonnant des mesures provisoires prise en vertu de l'article 70, paragraphe 1;

d) à respecter des engagements rendus juridiquement contraignants par voie de décision prise en vertu de l'article 71, paragraphe 1;

e) à respecter une décision prise en application de l'article 73, paragraphe 1, y compris, le cas échéant, les exigences qu'elle contient concernant le plan d'action visé à l'article 75.

2. Lorsque le fournisseur de la très grande plateforme en ligne ou du très grand moteur de recherche en ligne concerné ou une autre personne visée à l'article 67, paragraphe 1, ont satisfait à l'obligation pour l'exécution de laquelle l'astreinte a été infligée, la Commission peut fixer le montant définitif de l'astreinte à un chiffre inférieur à celui qui résulte de la décision initiale.

Article 77 - Prescription en matière d'imposition de sanctions

1. Les pouvoirs conférés à la Commission par les articles 74 et 76 sont soumis à un délai de prescription de cinq ans.

2. Le délai de prescription court à compter du jour où l'infraction a été commise. Toutefois, pour les infractions continues ou répétées, le délai de prescription ne court qu'à compter du jour où l'infraction prend fin.

3. Le délai de prescription en matière d'imposition d'amendes ou d'astreintes est interrompu par tout acte de la Commission ou du coordinateur pour les services numériques aux fins de l'enquête ou de la procédure relative à l'infraction. Constituent notamment des actes interrompant la prescription:

a) les demandes d'informations de la Commission ou d'un coordinateur pour les services numériques;

b) l'inspection;

c) l'ouverture d'une procédure par la Commission en vertu de l'article 66, paragraphe 1.

4. Un nouveau délai de prescription commence à courir à partir de chaque interruption. Toutefois, la prescription en matière d'imposition d'amendes ou d'astreintes est acquise au plus tard le jour où un délai égal au double du délai de prescription arrive à expiration sans

que la Commission ait prononcé une amende ou astreinte. Ce délai est prolongé de la période pendant laquelle le délai de prescription a été suspendu conformément au paragraphe 5.

5. La prescription en matière d'imposition d'amendes ou d'astreintes est suspendue aussi longtemps que la décision de la Commission fait l'objet d'une procédure pendante devant la Cour de justice de l'Union européenne.

Article 78 - Prescription en matière d'exécution des sanctions

1. Le pouvoir de la Commission d'exécuter les décisions prises en application des articles 74 et 76 est soumis à un délai de prescription de cinq ans.

2. Le délai de prescription court à compter du jour où la décision est devenue définitive.

3. Le délai de prescription en matière d'exécution des sanctions est interrompu:

   a) par la notification d'une décision modifiant le montant initial de l'amende ou de l'astreinte ou rejetant une demande tendant à obtenir une telle modification;

   b) par tout acte de la Commission ou d'un État membre agissant à la demande de la Commission, visant au recouvrement forcé de l'amende ou de l'astreinte.

4. Un nouveau délai de prescription commence à courir à partir de chaque interruption.

5. Le délai de prescription en matière d'exécution forcée des sanctions est suspendu:

   a) aussi longtemps qu'un délai de paiement est accordé;

   b) aussi longtemps que l'exécution forcée du paiement est suspendue en vertu d'une décision de la Cour de justice de l'Union européenne ou d'une décision d'une juridiction nationale.

Article 79 - Droit d'être entendu et droit d'accès au dossier

1. Avant d'adopter une décision au titre de l'article 73, paragraphe 1, de l'article 74 ou de l'article 76, la Commission donne au fournisseur de la très grande plateforme en ligne ou du très grand moteur de recherche en ligne concerné ou à une autre personne visée à l'article 67, paragraphe 1, l'occasion de faire connaître son point de vue sur:

   a) les constatations préliminaires de la Commission, y compris sur tout grief retenu par la Commission; et

   b) les mesures que la Commission peut avoir l'intention de prendre au vu des constatations préliminaires visées au point a).

2. Le fournisseur de la très grande plateforme en ligne ou du très grand moteur de recherche en ligne concerné ou une autre personne visée à l'article 67, paragraphe 1, peut présenter ses observations sur les constatations préliminaires de la Commission dans un délai raisonnable fixé par la Commission dans ses constatations préliminaires et qui ne peut être inférieur à quatorze jours.

3. La Commission ne fonde ses décisions que sur les griefs au sujet desquels les parties concernées ont pu faire valoir leurs observations.

4. Les droits de la défense des parties concernées sont pleinement respectés dans le déroulement de la procédure. Les parties ont le droit d'avoir accès au dossier de la Commission conformément aux modalités d'une divulgation négociée, sous réserve de l'intérêt légitime du fournisseur de la très grande plateforme en ligne ou du très grand moteur de recherche en ligne concerné ou d'une autre personne concernée à ce que leurs secrets d'affaires ne soient pas divulgués. La Commission est habilitée à adopter des décisions fixant ces modalités de divulgation en cas de désaccord entre les parties. Le droit d'accès au dossier de la Commission ne s'étend pas aux informations confidentielles et aux documents internes de la Commission, du comité, des coordinateurs pour les services numériques, d'autres autorités compétentes ou d'autres autorités publiques des États membres. En particulier, le droit d'accès ne s'étend pas à la correspondance entre la Commission et ces autorités. Aucune disposition du présent paragraphe n'empêche la Commission de divulguer et d'utiliser des informations nécessaires pour apporter la preuve d'une infraction.

5. Les informations recueillies par application des articles 67, 68 et 69 ne sont utilisées qu'aux fins du présent règlement.

Article 80- Publication des décisions

1. La Commission publie les décisions qu'elle adopte au titre de l'article 70, paragraphe 1, de l'article 71, paragraphe 1, et des articles 73 à 76. Cette publication mentionne le nom des parties intéressées et l'essentiel de la décision, y compris les sanctions imposées.

2. La publication tient compte des droits et intérêts légitimes du fournisseur de la très grande plateforme en ligne ou du très grand moteur de recherche en ligne concerné, de toute autre personne visée à l'article 67, paragraphe 1, et de tout tiers à ce que leurs informations confidentielles ne soient pas divulguées.

Article 81- Contrôle de la Cour de justice de l'Union européenne

Conformément à l'article 261 du traité sur le fonctionnement de l'Union européenne, la Cour de justice de l'Union européenne statue avec compétence de pleine juridiction sur les recours formés contre les décisions par lesquelles la Commission inflige des amendes ou des astreintes. Elle peut supprimer, réduire ou majorer l'amende ou l'astreinte infligée.

Article 82 - Demandes de restrictions d'accès et coopération avec les juridictions nationales

1. Lorsque tous les pouvoirs au titre de la présente section pour parvenir à la cessation d'une infraction au présent règlement ont été épuisés, que l'infraction persiste et entraîne un préjudice grave ne pouvant pas être évité via l'exercice d'autres pouvoirs prévus par le droit de l'Union ou le droit national, la Commission peut demander au coordinateur pour les services numériques de l'État membre d'établissement du fournisseur de la très grande plateforme en ligne ou du très grand moteur de recherche en ligne concerné d'agir conformément à l'article 51, paragraphe 3.

Avant d'adresser une telle demande au coordinateur pour les services numériques, la Commission invite les parties intéressées à soumettre des observations écrites dans un délai qui ne peut être inférieur à quatorze jours ouvrables, en décrivant les mesures qu'elle entend demander et en identifiant le ou les destinataires prévus.

2. Lorsque l'application cohérente du présent règlement le justifie, la Commission, agissant d'office, peut soumettre des observations écrites à l'autorité judiciaire compétente visée à l'article 51, paragraphe 3. Avec l'autorisation de l'autorité judiciaire en question, elle peut aussi présenter des observations orales.

Aux seules fins de lui permettre de préparer ses observations, la Commission peut solliciter l'autorité judiciaire afin qu'elle lui transmette ou lui fasse transmettre tout document nécessaire à l'appréciation de l'affaire.

3. Lorsqu'une juridiction nationale statue sur une question qui fait déjà l'objet d'une décision adoptée par la Commission au titre du présent règlement, cette juridiction nationale ne prend aucune décision allant à l'encontre de la décision de la Commission. Les juridictions nationales évitent également de prendre des décisions qui iraient à l'encontre d'une décision envisagée par la Commission dans une procédure qu'elle a intentée au titre du présent règlement. À cette fin, la juridiction nationale peut évaluer s'il est nécessaire de suspendre sa procédure. Cette disposition est sans préjudice de l'article 267 du traité sur le fonctionnement de l'Union européenne.

Article 83 - Actes d'exécution relatifs à l'intervention de la Commission

En ce qui concerne l'intervention de la Commission au titre de la présente section, la Commission peut adopter des actes d'exécution établissant les modalités pratiques pour:

a) les procédures au titre des articles 69 et 72;

b) les auditions prévues à l'article 79;

c) la divulgation négociée d'informations prévue à l'article 79.

Avant d'adopter une disposition en vertu du premier alinéa du présent article, la Commission en publie le projet et invite toutes les parties intéressées à lui soumettre leurs observations dans un délai qu'elle fixe et qui ne peut être inférieur à un mois. Ces actes d'exécution sont adoptés en conformité avec la procédure consultative visée à l'article 88.

SECTION 5

Dispositions communes relatives à l'exécution

Article 84 - Secret professionnel

Sans préjudice de l'échange et de l'utilisation des informations visées dans le présent chapitre, la Commission, le comité, les autorités compétentes des États membres et leurs fonctionnaires, agents et les autres personnes travaillant sous leur supervision respectifs, ainsi que toute autre personne physique ou morale impliquée, dont les auditeurs et experts nommés en vertu de l'article 72, paragraphe 2, sont tenus de ne pas divulguer les informations qu'ils

ont recueillies ou échangées au titre du présent règlement et qui, par leur nature, sont couvertes par le secret professionnel.

Article 85 - Système de partage d'informations

1. La Commission met en place et maintient un système de partage d'informations fiable et sûr facilitant les communications entre les coordinateurs pour les services numériques, la Commission et le comité. D'autres autorités compétentes peuvent se voir accorder l'accès à ce système, lorsque cela s'avère nécessaire pour l'accomplissement des tâches qui leur sont confiées conformément au présent règlement.

2. Les coordinateurs pour les services numériques, la Commission et le comité utilisent le système de partage d'informations pour toutes les communications au titre du présent règlement.

3. La Commission adopte des actes d'exécution établissant les modalités pratiques et opérationnelles du fonctionnement du système de partage d'informations et de son interopérabilité avec d'autres systèmes pertinents. Ces actes d'exécution sont adoptés en conformité avec la procédure consultative visée à l'article 88.

Article 86 - Représentation

1. Sans préjudice de la directive (UE) 2020/1828 ou de tout autre type de représentation au titre du droit national, les destinataires de services intermédiaires ont à tout le moins le droit de mandater un organisme, une organisation ou une association pour exercer les droits conférés par le présent règlement pour leur compte, pour autant que cet organisme, cette organisation ou cette association remplisse toutes les conditions suivantes:

a) il opère sans but lucratif;

b) il a été régulièrement constitué, conformément au droit d'un État membre;

c) ses objectifs statutaires comprennent un intérêt légitime à assurer le respect du présent règlement.

2. Les fournisseurs de plateformes en ligne prennent les mesures techniques et organisationnelles nécessaires pour veiller à ce que les plaintes déposées par les organismes, organisations ou associations visés au paragraphe 1 du présent article au nom des destinataires du service à l'aide des mécanismes prévus à l'article 20, paragraphe 1, soient traitées et donnent lieu à des décisions de manière prioritaire et sans retard injustifié.

SECTION 6

Actes délégués et actes d'exécution

Article 87 - Exercice de la délégation

1. Le pouvoir d'adopter des actes délégués conféré à la Commission est soumis aux conditions fixées au présent article.

2. La délégation de pouvoir visée aux articles 24, 33, 37, 40 et 43 est conférée à la Commission pour une période de cinq ans à compter du 16 novembre 2022. La Commission élabore un rapport relatif à la délégation de pouvoir au plus tard neuf mois avant la fin de la période de cinq ans. La délégation de pouvoir est tacitement prorogée pour des périodes d'une durée identique, sauf si le Parlement européen ou le Conseil s'oppose à cette prorogation trois mois au plus tard avant la fin de chaque période.

3. La délégation de pouvoir visée aux articles 24, 33, 37, 40 et 43 peut être révoquée à tout moment par le Parlement européen ou le Conseil. La décision de révocation met fin à la délégation de pouvoir qui y est précisée. La révocation prend effet le jour suivant celui de la publication de ladite décision au Journal officiel de l'Union européenne ou à une date ultérieure qui est précisée dans ladite décision. Elle ne porte pas atteinte à la validité des actes délégués déjà en vigueur.

4. Avant l'adoption d'un acte délégué, la Commission consulte les experts désignés par chaque État membre, conformément aux principes définis dans l'accord interinstitutionnel du 13 avril 2016"Mieux légiférer".

5. Aussitôt qu'elle adopte un acte délégué, la Commission le notifie simultanément au Parlement européen et au Conseil.

6. Un acte délégué adopté en vertu des articles 24, 33, 37, 40 et 43 n'entre en vigueur que si le Parlement européen ou le Conseil n'a pas exprimé d'objections dans un délai de trois mois à compter de la notification de cet acte au Parlement européen et au Conseil ou si, avant l'expiration de ce délai, le Parlement européen et le Conseil ont tous deux informé la Commission de leur intention de ne pas exprimer d'objections. Ce délai est prolongé de trois mois à l'initiative du Parlement européen ou du Conseil.

Article 88 - Comité

1. La Commission est assistée par un comité (ci-après dénommé "comité pour les services numériques"). Ledit comité est un comité au sens du règlement (UE) n° 182/2011.

2. Lorsqu'il est fait référence au présent paragraphe, l'article 4 du règlement (UE) n° 182/2011 s'applique.

CHAPITRE V

DISPOSITIONS FINALES

Article 89 - Modifications de la directive 2000/31/CE

1. Les articles 12 à 15 de la directive 2000/31/CE sont supprimés.

2. Les références aux articles 12 à 15 de la directive 2000/31/CE s'entendent comme étant faites respectivement aux articles 4, 5, 6 et 8 du présent règlement.

Article 90 - Modification de la directive (UE) 2020/1828

À l'annexe I de la directive (UE) 2020/1828, le point suivant est ajouté:

“68)

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) (JO L 277 du 27.10.2022, p. 1).”

Article 91- Réexamen

1. Au plus tard le 18 février 2027, la Commission évalue l’effet potentiel du présent règlement sur le développement et la croissance économique des petites et moyennes entreprises et présente un rapport à cet égard au Parlement européen, au Conseil et au Comité économique et social européen.

Au plus tard le 17 novembre 2025, la Commission évalue les éléments suivants et fait rapport à ce sujet au Parlement européen, au Conseil et au Comité économique et social:

a) l’application de l’article 33, y compris l’éventail des fournisseurs de services intermédiaires couverts par les obligations prévues au chapitre III, section 5, du présent règlement;

b) la manière dont le présent règlement interagit avec d’autres actes juridiques, en particulier les actes visés à l’article 2, paragraphes 3 et 4.

2. Au plus tard le 17 novembre 2027, puis tous les cinq ans, la Commission évalue le présent règlement et fait rapport au Parlement européen, au Conseil et au Comité économique et social européen.

Ce rapport porte en particulier sur:

a) L’application du paragraphe 1, deuxième alinéa, points a) et b);

b) La contribution du présent règlement à l’approfondissement et au fonctionnement efficace du marché intérieur des services intermédiaires, notamment en ce qui concerne la fourniture transfrontalière de services numériques;

c) L’application des articles 13, 16, 20, 21, 45 et 46;

d) La portée des obligations pesant sur les petites entreprises et les microentreprises;

e) L’efficacité des mécanismes de surveillance et d’exécution;

f) l’incidence sur le respect du droit à la liberté d’expression et d’information.

3. Le rapport visé aux paragraphes 1 et 2 est accompagné, le cas échéant, d’une proposition de modification du présent règlement.

4. La Commission évalue également, dans le rapport visé au paragraphe 2 du présent article, les rapports d’activité annuels des coordinateurs pour les services numériques présentés à la

Commission et au comité au titre de l'article 55, paragraphe 1, et en rend compte dans ledit rapport.

5. Aux fins du paragraphe 2, les États membres et le comité fournissent à la Commission les informations qu'elle demande.

6. Lorsqu'elle procède aux évaluations visées au paragraphe 2, la Commission tient compte des positions et des conclusions du Parlement européen, du Conseil, et d'autres organismes ou sources pertinents et prête une attention particulière aux petites et moyennes entreprises et à la position de nouveaux concurrents.

7. Au plus tard le 18 février 2027, la Commission, après avoir consulté le comité, procède à une évaluation du fonctionnement du comité et de l'application de l'article 43, et elle fait rapport au Parlement européen, au Conseil et au Comité économique et social européen, en tenant compte des premières années d'application du règlement. Sur la base des conclusions et en tenant le plus grand compte de l'avis du comité, le rapport est accompagné, le cas échéant, d'une proposition de modification du présent règlement en ce qui concerne la structure du comité.

Article 92- Application anticipée à l'égard des fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne

Le présent règlement s'applique aux fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne désignés en vertu de l'article 33, paragraphe 4, quatre mois après la notification adressée au fournisseur concerné visée à l'article 33, paragraphe 6, lorsque cette date est antérieure au 17 février 2024.

Article 93 - Entrée en vigueur et application

1. Le présent règlement entre en vigueur le vingtième jour suivant celui de sa publication au Journal officiel de l'Union européenne.

2. Le présent règlement est applicable à partir du 17 février 2024.

Toutefois, l'article 24, paragraphes 2, 3 et 6, l'article 33, paragraphes 3 à 6, l'article 37, paragraphe 7, l'article 40, paragraphe 13, l'article 43 et le chapitre IV, sections 4, 5 et 6, sont applicables à partir du 16 novembre 2022.

Le présent règlement est obligatoire dans tous ses éléments et directement applicable dans tout État membre.

Fait à Strasbourg, le 19 octobre 2022.

Par le Parlement européen

La présidente

R. METSOLA

Par le Conseil

Le président

M. BEK

Annexe 2 : Journal officiel de l'Union européenne – règlementation DMA

Article premier

Objet et champ d'application

1. L'objectif du présent règlement est de contribuer au bon fonctionnement du marché intérieur, en établissant des règles harmonisées visant à garantir à toutes les entreprises la contestabilité et l'équité des marchés dans le secteur numérique de l'Union là où des contrôleurs d'accès sont présents, au profit des entreprises utilisatrices et des utilisateurs finaux.

2. Le présent règlement s'applique aux services de plateforme essentiels fournis ou proposés par des contrôleurs d'accès à des entreprises utilisatrices établies dans l'Union ou à des utilisateurs finaux établis ou situés dans l'Union, quel que soit le lieu d'établissement ou de résidence des contrôleurs d'accès et quel que soit le droit par ailleurs applicable à la fourniture des services.

3. Le présent règlement ne s'applique pas aux marchés liés:

a) aux réseaux de communications électroniques au sens de l'article 2, point 1), de la directive (UE) 2018/1972;

b) aux services de communications électroniques au sens de l'article 2, point 4), de la directive (UE) 2018/1972, autres que ceux liés aux services de communications interpersonnelles non fondés sur la numérotation.

4. En ce qui concerne les services de communications interpersonnelles au sens de l'article 2, point 5), de la directive (UE) 2018/1972, le présent règlement est sans préjudice des pouvoirs et responsabilités confiés aux autorités de régulation nationales et autres autorités compétentes en vertu de l'article 61 de ladite directive.

5. Afin d'éviter la fragmentation du marché intérieur, les États membres n'imposent pas d'obligations supplémentaires aux contrôleurs d'accès par voie législative, réglementaire ou de mesures administratives aux fins de garantir la contestabilité et l'équité des marchés. Aucune disposition du présent règlement n'empêche les États membres d'imposer aux entreprises, y compris les entreprises fournissant des services de plateforme essentiels, des obligations sur des points ne relevant pas du champ d'application du présent règlement, pour autant que ces obligations soient compatibles avec le droit de l'Union et ne résultent pas du fait que les entreprises concernées ont le statut d'un contrôleur d'accès au sens du présent règlement.

6. Le présent règlement est sans préjudice de l'application des articles 101 et 102 du traité sur le fonctionnement de l'Union européenne. Il est également sans préjudice de l'application :

a) des règles de concurrence nationales interdisant les accords anticoncurrentiels, les décisions d'associations d'entreprises, les pratiques concertées et les abus de position dominante ;

b) des règles de concurrence nationales interdisant d'autres formes de comportement unilatéral, dans la mesure où elles s'appliquent à des entreprises autres que les contrôleurs d'accès ou reviennent à imposer des obligations supplémentaires aux contrôleurs d'accès; et

c)du règlement (CE) no 139/2004 du Conseil (23) et des règles nationales relatives au contrôle des concentrations.

7. Les autorités nationales ne prennent aucune décision qui va à l'encontre d'une décision adoptée par la Commission en vertu du présent règlement. La Commission et les États membres travaillent en étroite coopération et coordonnent leurs mesures d'exécution en se fondant sur les principes établis aux articles 37 et 38.

Article 2

Aux fins du présent règlement, on entend par:

1**) «contrôleur** d'accès»: une entreprise fournissant des services de plateforme essentiels, désignée conformément à l'article 3;

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) navigateurs internet;

h) assistants virtuels;

i) services d'informatique en nuage;

j)services de publicité en ligne, y compris tout réseau publicitaire, échange publicitaire et autre service d'intermédiation publicitaire, fourni par une entreprise qui met à disposition n'importe lequel des services de plateforme essentiels énumérés aux points a) à i);

3**) «service de la société de l'information**» : tout service au sens de l'article 1er, paragraphe 1, point b), de la directive (UE) 2015/1535;

4) «**secteur numérique»**: le secteur des produits et services fournis au moyen ou par l'intermédiaire de services de la société de l'information;

5**) «services d'intermédiation en ligne**»: les services d'intermédiation en ligne au sens de l'article 2, point 2), du règlement (UE) 2019/1150;

6) **«moteur de recherche en ligne»:** un moteur de recherche en ligne au sens de l'article 2, point 5), du règlement (UE) 2019/1150;

7) **«service de réseaux sociaux en ligne**»: une plateforme permettant aux utilisateurs finaux de se connecter ainsi que de communiquer entre eux, de partager des contenus et de découvrir d'autres utilisateurs et d'autres contenus, sur plusieurs appareils et, en particulier, au moyen de conversations en ligne (chats), de publications (posts), de vidéos et de recommandations;

8**) «service de plateformes de partage de vidéos**»: un service de plateformes de partage de vidéos au sens de l'article 1er, paragraphe 1, point a bis), de la directive 2010/13/UE;

9) **«service de communications interpersonnelles non fondé sur la numérotation**»: un service de communications interpersonnelles non fondé sur la numérotation au sens de l'article 2, point 7), de la directive (UE) 2018/1972;

10) **«système d'exploitation»:** un logiciel système qui contrôle les fonctions de base du matériel informatique ou du logiciel et permet d'y faire fonctionner des applications logicielles;

11) **«navigateur internet»**: une application logicielle qui permet aux utilisateurs finaux d'accéder à des contenus internet hébergés sur des serveurs connectés à des réseaux tels que l'internet, y compris les navigateurs internet autonomes, ainsi que les navigateurs internet intégrés ou inclus dans un logiciel ou équivalent, et d'interagir avec ces contenus;

12) **«assistant virtuel»:** un logiciel qui peut traiter des demandes, des tâches ou des questions, notamment celles fondées sur des données d'entrée sonores, visuelles ou écrites, de gestes ou de mouvements, et qui, sur la base de ces demandes, tâches ou questions, donne accès à d'autres services ou contrôle des appareils connectés physiques;

13) **«service d'informatique en nuage»:** un service d'informatique en nuage au sens de l'article 4, point 19), de la directive (UE) 2016/1148 du Parlement européen et du Conseil (24);

14) **«boutique d'applications logicielles»:** un type de services d'intermédiation en ligne qui se concentre sur les applications logicielles en tant que produit ou service intermédié;

15**) «application logicielle**»: tout produit ou service numérique fonctionnant sur un système d'exploitation;

16) «**service de paiement**»: un service de paiement au sens de l'article 4, point 3), de la directive (UE) 2015/2366;

17) **«service technique à l'appui d'un service de paiement»**: un service au sens de l'article 3, point j), de la directive (UE) 2015/2366;

18) **«système de paiement pour les achats intégrés à des applications»:** une application logicielle, un service ou une interface utilisateur qui facilite les achats de contenu numérique ou de services numériques dans une application logicielle, y compris en termes de contenu, d'abonnements, de caractéristiques ou de fonctionnalité, ainsi que les paiements pour de tels achats;

19) **«service d'identification»:** un type de service fourni avec ou à l'appui des services de plateforme essentiels permettant toute sorte de vérification de l'identité des utilisateurs finaux ou des entreprises utilisatrices, indépendamment de la technologie utilisée;

20) **«utilisateur final» :** toute personne physique ou morale utilisant des services de plateforme essentiels autrement qu'en tant qu'entreprise utilisatrice;

21) «**entreprise utilisatrice» :** toute personne physique ou morale agissant à titre commercial ou professionnel qui utilise des services de plateforme essentiels aux fins ou dans le cadre de la fourniture de biens ou de services à des utilisateurs finaux;

22**) «classement**»: la priorité relative accordée aux biens ou services proposés par le biais de services d'intermédiation en ligne, de services de réseaux sociaux en ligne, de services de plateformes de partage de vidéos ou d'assistants virtuels, ou la pertinence reconnue aux résultats de recherche par les moteurs de recherche en ligne, tels qu'ils sont présentés, organisés ou communiqués par les entreprises fournissant des services d'intermédiation en ligne, des services de plateformes de partage de vidéos, des assistants virtuels ou des moteurs de recherche en ligne, indépendamment des moyens technologiques utilisés pour une telle présentation, organisation ou communication et indépendamment du fait qu'un seul résultat soit ou non présenté ou communiqué;

23) **«résultats de recherche»:** toute information, sous quelque format que ce soit, y compris des données textuelles, graphiques, vocales ou autres, renvoyées en réponse à une recherche, et en rapport avec celle-ci, que l'information renvoyée soit un résultat payant ou non, une réponse directe ou tout produit, service ou renseignement proposé en lien avec les résultats organiques, affiché en même temps que ceux-ci ou partiellement ou entièrement intégré dans ceux-ci;

24) **«données»:** toute représentation numérique d'actes, de faits ou d'informations et toute compilation de ces actes, faits ou informations, notamment sous la forme d'enregistrements sonores, visuels ou audiovisuels;

25) **«données à caractère personnel**»: les données à caractère personnel au sens de l'article 4, point 1), du règlement (UE) 2016/679;

26) **«données à caractère non personnel»:** les données autres que les données à caractère personnel;

27) **«entreprise»:** une entité exerçant une activité économique, indépendamment de son statut juridique et de son mode de financement, y compris toutes les entreprises liées ou connectées formant un groupe par l'intermédiaire du contrôle direct ou indirect d'une entreprise par une autre;

28) **«contrôle**»: la possibilité d'exercer une influence déterminante sur l'activité d'une entreprise, au sens de l'article 3, paragraphe 2, du règlement (CE) no 139/2004;

29) «**interopérabilité»**: la capacité d'échanger des informations et d'utiliser mutuellement les informations échangées par le biais d'interfaces ou d'autres solutions, de telle sorte que tous les éléments du matériel informatique ou des logiciels fonctionnent de toutes les manières dont elles sont censées fonctionner avec d'autres matériels informatiques et logiciels ainsi qu'avec les utilisateurs;

30) **«chiffre d'affaires»:** le montant réalisé par une entreprise au sens de l'article 5,

31) **«profilage»:** le profilage au sens de l'article 4, point 4), du règlement (UE) 2016/679;

32**) «consentement**»: le consentement au sens de l'article 4, point 11), du règlement (UE) 2016/679;

33) **« juridiction nationale** »: toute juridiction d'un État membre au sens de l'article 267 du traité sur le fonctionnement de l'Union européenne.

CHAPITRE II
CONTRÔLEURS D'ACCÈS
Article 3
Désignation des contrôleurs d'accès

1. Une entreprise est désignée comme étant un contrôleur d'accès si:

   a) elle a un poids important sur le marché intérieur;

   b) elle fournit un service de plateforme essentiel qui constitue un point d'accès majeur permettant aux entreprises utilisatrices d'atteindre leurs utilisateurs finaux; et

   c) elle jouit d'une position solide et durable, dans ses activités, ou jouira, selon toute probabilité, d'une telle position dans un avenir proche.

2. Une entreprise est réputée satisfaire aux exigences respectives du paragraphe 1:

   a) en ce qui concerne le paragraphe 1, point a), si elle a réalisé un chiffre d'affaires annuel dans l'Union supérieur ou égal à 7,5 milliards d'euros au cours de chacun des trois derniers exercices, ou si sa capitalisation boursière moyenne ou sa juste valeur marchande équivalente a atteint au moins 75 milliards d'euros au cours du dernier exercice, et qu'elle fournit le même service de plateforme essentiel dans au moins trois États membres;
   b) en ce qui concerne le paragraphe 1, point b), si elle fournit un service de plateforme essentiel qui, au cours du dernier exercice, a compté au moins 45 millions d'utilisateurs finaux actifs par mois établis ou situés dans l'Union et au moins 10 000 entreprises utilisatrices actives par an établies dans l'Union, faisant l'objet d'une identification et de calculs conformément à la méthode et aux indicateurs définis dans l'annexe;

   c) en ce qui concerne le paragraphe 1, point c), si les seuils visés au point b) du présent paragraphe ont été atteints au cours de chacun des trois derniers exercices.

3. Lorsqu'une entreprise fournissant des services de plateforme essentiels atteint l'ensemble des seuils mentionnés au paragraphe 2, elle en informe la Commission sans tarder et, en tout état de cause, dans les deux mois qui suivent après que ces seuils ont été atteints et lui fournit les informations pertinentes visées au paragraphe 2. Cette notification inclut les informations pertinentes visées au paragraphe 2 pour chacun des services de plateforme essentiels de l'entreprise qui atteint les seuils mentionnés au paragraphe 2, point b). Lorsqu'un autre service de plateforme essentiel fourni par l'entreprise qui a précédemment été désignée comme étant un contrôleur d'accès atteint les seuils mentionnés au paragraphe 2, points b) et c), cette entreprise en informe la Commission dans les deux mois qui suivent le respect de ces seuils.

Lorsque l'entreprise fournissant le service de plateforme essentiel n'informe pas la Commission conformément au premier alinéa du présent paragraphe et qu'elle ne parvient pas à fournir, dans le délai fixé par la Commission dans la demande de renseignements visée à

l'article 21, tous les renseignements pertinents dont la Commission a besoin pour désigner l'entreprise concernée en tant que contrôleur d'accès en vertu du paragraphe 4 du présent article, la Commission conserve le droit de désigner cette entreprise en tant que contrôleur d'accès, sur la base des informations dont elle dispose.

Lorsque l'entreprise fournissant des services de plateforme essentiels se conforme à la demande de renseignement en vertu du deuxième alinéa du présent paragraphe ou que les renseignements sont fournis après l'expiration du délai visé à cet alinéa, la Commission applique la procédure prévue au paragraphe 4.

4. La Commission désigne comme étant un contrôleur d'accès, sans retard indu et au plus tard dans un délai de 45 jours ouvrables après avoir reçu toutes les informations visées au paragraphe 3, une entreprise fournissant des services de plateforme essentiels qui atteint tous les seuils mentionnés au paragraphe 2.

5. L'entreprise fournissant des services de plateforme essentiels peut présenter, avec sa notification, des arguments suffisamment étayés pour démontrer que, exceptionnellement, bien qu'elle atteigne tous les seuils prévus au paragraphe 2 et en raison des circonstances dans lesquelles le service de plateforme essentiel concerné opère, elle ne satisfait pas aux exigences énumérées au paragraphe 1.

Lorsque la Commission estime que les arguments présentés en vertu du premier alinéa par l'entreprise fournissant des services de plateforme essentiels ne sont pas suffisamment étayés parce qu'ils ne remettent manifestement pas en cause les présomptions énoncées au paragraphe 2 du présent article, elle peut rejeter ces arguments dans le délai visé au paragraphe 4, sans appliquer la procédure prévue à l'article 17, paragraphe 3.

Lorsque l'entreprise fournissant des services de plateforme essentiels présente de tels arguments suffisamment étayés, remettant manifestement en cause les présomptions mentionnées au paragraphe 2 du présent article, la Commission peut, nonobstant le premier alinéa du présent paragraphe et dans le délai visé au paragraphe 4 du présent article, ouvrir la procédure prévue à l'article 17, paragraphe 3.

Si la Commission conclut que l'entreprise fournissant des services de plateforme essentiels n'a pas été en mesure de démontrer que les services de plateforme essentiels qu'elle fournit ne satisfont pas aux exigences du paragraphe 1 du présent article, elle désigne cette entreprise comme étant un contrôleur d'accès conformément à la procédure prévue à l'article 17, paragraphe 3.

6. La Commission est habilitée à adopter des actes délégués conformément à l'article 49 afin de compléter le présent règlement en précisant la méthode utilisée pour déterminer si les seuils quantitatifs fixés au paragraphe 2 du présent article sont atteints, et d'adapter régulièrement ladite méthode, le cas échéant, aux évolutions du marché et de la technologie.

7. La Commission est habilitée à adopter des actes délégués conformément à l'article 49 afin de modifier le présent règlement en mettant à jour la méthode et la liste des indicateurs définies dans l'annexe.

8. La Commission désigne comme étant un contrôleur d'accès, conformément à la procédure prévue à l'article 17, toute entreprise fournissant des services de plateforme essentiels qui

satisfait à chacune des exigences visées au paragraphe 1 du présent article, mais n'atteint pas chacun des seuils mentionnés au paragraphe 2 du présent article.

À cette fin, la Commission tient compte de tout ou partie des éléments ci-après, pour autant qu'ils soient pertinents pour l'entreprise considérée fournissant des services de plateforme essentiels:

a) La taille, y compris le chiffre d'affaires et la capitalisation boursière, les activités et la position de ladite entreprise;

b) Le nombre d'entreprises utilisatrices qui font appel au service de plateforme essentiel pour atteindre des utilisateurs finaux et le nombre d'utilisateurs finaux;

c) Les effets de réseau et les avantages tirés des données, en particulier en ce qui concerne l'accès aux données à caractère personnel et non personnel et la collecte de ces données par ladite entreprise, ou les capacités d'analyse de cette dernière;

d) Tout effet d'échelle et de gamme dont bénéficie l'entreprise, y compris en ce qui concerne les données et, le cas échéant, ses activités en dehors de l'Union;

e) La captivité des entreprises utilisatrices ou des utilisateurs finaux, y compris les coûts de changement et les biais comportementaux qui réduisent la capacité des entreprises utilisatrices et des utilisateurs finaux à changer de fournisseur ou à opter pour un multi hébergement;

f) Une structure d'entreprise conglomérale ou l'intégration verticale de cette entreprise, permettant par exemple à celle-ci de pratiquer des subventions croisées, de combiner des données provenant de différentes sources ou de tirer parti de sa position; ou

g) D'autres caractéristiques structurelles des entreprises ou des services.

Dans le cadre de la réalisation de son appréciation au titre du présent paragraphe, la Commission tient compte de l'évolution prévisible en relation avec les éléments énumérés au deuxième alinéa, y compris tout projet de concentration faisant intervenir une autre entreprise fournissant des services de plateforme essentiels ou tout autre service dans le secteur numérique ou permettant la collecte de données.

Si une entreprise fournissant un service de plateforme essentiel qui n'atteint pas les seuils quantitatifs visés au paragraphe 2 ne se conforme pas de manière substantielle aux mesures d'enquête ordonnées par la Commission et si ce manquement persiste après que cette entreprise a été invitée à s'y conformer dans un délai raisonnable et à soumettre ses observations, la Commission peut désigner cette entreprise comme étant un contrôleur d'accès sur la base des faits dont dispose la Commission.

9. Pour chaque entreprise désignée comme étant un contrôleur d'accès en vertu du paragraphe 4 ou 8, la Commission énumère dans la décision de désignation les services de plateforme essentiels concernés qui sont fournis au sein de cette entreprise et qui constituent, individuellement, des points d'accès majeurs permettant aux entreprises utilisatrices d'atteindre les utilisateurs finaux, comme indiqué au paragraphe 1, point b).

10. Le contrôleur d'accès se conforme aux obligations prévues aux articles 5, 6 et 7 dans les six mois suivant l'énumération d'un service de plateforme essentiel dans la décision de désignation conformément au paragraphe 9 du présent article.

Article 4

Réexamen du statut de contrôleur d'accès

1. La Commission peut, sur demande ou de sa propre initiative, revoir, modifier ou abroger à tout moment une décision de désignation adoptée au titre de l'article 3 pour l'une des raisons suivantes :

a) l'un des faits sur lesquels la décision de désignation repose subit un changement important ;

b) la décision de désignation repose sur des informations incomplètes, inexactes ou dénaturées.

2. La Commission réexamine régulièrement, et au moins tous les trois ans, si les contrôleurs d'accès continuent de satisfaire aux exigences fixées à l'article 3, paragraphe 1. Ce réexamen détermine également s'il faut modifier la liste des services de plateforme essentiels du contrôleur d'accès qui constituent, individuellement, des points d'accès majeurs permettant aux entreprises utilisatrices d'atteindre les utilisateurs finaux, comme indiqué à l'article 3, paragraphe 1, point b). Ces réexamens n'ont pas d'effet suspensif sur les obligations du contrôleur d'accès.

La Commission examine également au moins une fois par an si de nouvelles entreprises fournissant des services de plateforme essentiels satisfont à ces exigences.

Si la Commission constate, sur la base des examens menés conformément au premier alinéa, que les faits sur lesquels repose la désignation des entreprises fournissant des services de plateforme essentiels comme contrôleurs d'accès ont évolué, elle adopte une décision confirmant, modifiant ou abrogeant la décision de désignation.

3. La Commission publie et tient à jour de façon continue une liste des contrôleurs d'accès et la liste des services de plateforme essentiels pour lesquels ils doivent se conformer aux obligations prévues au chapitre III**.**

CHAPITRE III

PRATIQUES DES CONTRÔLEURS D'ACCÈS QUI LIMITENT LA CONTESTABILITÉ OU SONT DÉLOYALES

Article 5

Obligations incombant aux contrôleurs d'accès

1. Le contrôleur d'accès se conforme à toutes les obligations énoncées au présent article pour chacun de ses services de plateforme essentiels énumérés dans la décision de désignation conformément à l'article 3, paragraphe 9.

2. Tout contrôleur d'accès est tenu de ne pas:

a) traiter, aux fins de la fourniture de services de publicité en ligne, les données à caractère personnel des utilisateurs finaux qui recourent à des services de tiers utilisant des services de plateforme essentiels fournis par le contrôleur d'accès;

b) combiner les données à caractère personnel provenant du service de plateforme essentiel concerné avec les données à caractère personnel provenant de tout autre service de plateforme essentiel ou de tout autre service fourni par le contrôleur d'accès, ni avec des données à caractère personnel provenant de services tiers;

c) utiliser de manière croisée les données à caractère personnel provenant du service de plateforme essentiel concerné dans le cadre d'autres services fournis séparément par le contrôleur d'accès, y compris d'autres services de plateforme essentiels, et inversement; et

d) inscrire les utilisateurs finaux à d'autres services du contrôleur d'accès dans le but de combiner des données à caractère personnel,

à moins que ce choix précis ait été présenté à l'utilisateur final et que ce dernier ait donné son consentement au sens de l'article 4, point 11), et de l'article 7 du règlement (UE) 2016/679.

Lorsque le consentement donné aux fins du premier alinéa a été refusé ou retiré par l'utilisateur final, le contrôleur d'accès ne réitère pas sa demande de consentement pour la même finalité plus d'une fois par période d'un an.

Le présent paragraphe est sans préjudice de la possibilité pour le contrôleur d'accès de se fonder sur l'article 6, paragraphe 1, points c), d) et e), du règlement (UE) 2016/679, le cas échéant.

3. Le contrôleur d'accès n'empêche pas les entreprises utilisatrices de proposer les mêmes produits ou services aux utilisateurs finaux au moyen de services d'intermédiation en ligne tiers ou de leur propre canal de vente directe en ligne à des prix ou conditions différents de ceux qui sont proposés par les services d'intermédiation en ligne du contrôleur d'accès.

4. Le contrôleur d'accès permet aux entreprises utilisatrices de communiquer et de promouvoir leurs offres gratuitement, y compris à des conditions différentes, auprès des utilisateurs finaux acquis grâce à son service de plateforme essentiel ou via d'autres canaux, 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.

5. Le contrôleur d'accès permet aux utilisateurs finaux, par l'intermédiaire de ses services de plateforme essentiels, 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, y compris lorsque ces utilisateurs finaux ont acquis de tels éléments auprès des entreprises utilisatrices concernées sans avoir recours aux services de plateforme essentiels du contrôleur d'accès.

6. Le contrôleur d'accès n'empêche ni ne restreint directement ou indirectement la possibilité pour les entreprises utilisatrices ou les utilisateurs finaux de faire part à toute autorité publique compétente, y compris les juridictions nationales, de tout problème de non-respect, par le contrôleur d'accès, du droit de l'Union ou national pertinent dans le cadre des pratiques de ce dernier. Cela s'entend sans préjudice du droit des entreprises

utilisatrices et des contrôleurs d'accès d'établir, dans leurs accords, les conditions d'utilisation de mécanismes légaux de traitement des plaintes.

7. Le contrôleur d'accès n'exige pas des utilisateurs finaux qu'ils utilisent, ni des entreprises utilisatrices qu'elles utilisent, proposent ou interagissent avec un service d'identification, un navigateur internet ou un service de paiement, ou un service technique qui appuie la fourniture des services de paiement, tels que des systèmes de paiement destinés aux achats dans des applications, de ce contrôleur d'accès dans le cadre des services fournis par les entreprises utilisatrices en ayant recours aux services de plateforme essentiels de ce contrôleur d'accès.

8. Le contrôleur d'accès n'exige pas des entreprises utilisatrices ou des utilisateurs finaux qu'ils s'abonnent ou s'enregistrent à tout autre service de plateforme essentiel énuméré dans la décision de désignation conformément à l'article 3, paragraphe 9, ou atteignant les seuils visés à l'article 3, paragraphe 2, point b), comme condition pour être en mesure d'utiliser l'un des services de plateforme essentiels de ce contrôleur d'accès énumérés en vertu dudit article, d'y accéder, de s'y inscrire ou de s'y enregistrer.

9. Le contrôleur d'accès communique quotidiennement à chaque annonceur à qui il fournit des services de publicité en ligne, ou aux tiers autorisés par les annonceurs, à la demande de l'annonceur, des informations gratuites relatives à chaque publicité mise en ligne par l'annonceur, en ce qui concerne:

a) le prix et les frais payés par cet annonceur, y compris les déductions et suppléments éventuels, pour chacun des services de publicité en ligne concernés fournis par le contrôleur d'accès;
b) la rémunération perçue par l'éditeur, y compris les déductions et suppléments éventuels, sous réserve du consentement de l'éditeur; et
c) les mesures quantitatives à partir desquelles chacun des prix, frais et rémunérations est calculé.

Dans le cas où un éditeur ne consent pas au partage d'informations sur la rémunération perçue, comme visé au point b) du premier alinéa, le contrôleur d'accès fournit gratuitement à chaque annonceur des informations sur la rémunération moyenne quotidienne perçue par cet éditeur, y compris les déductions et suppléments éventuels, pour les publicités concernées.

10. Le contrôleur d'accès communique quotidiennement à chaque éditeur à qui il fournit des services de publicité en ligne, ou aux tiers autorisés par les éditeurs, à la demande de l'éditeur, des informations gratuites relatives à chaque publicité affichée dans l'inventaire de l'éditeur, en ce qui concerne:

a) la rémunération perçue et les frais payés par cet éditeur, y compris les déductions et suppléments éventuels, pour chacun des services de publicité en ligne concernés fournis par le contrôleur d'accès;

b) le prix payé par l'annonceur, y compris les déductions et suppléments éventuels, sous réserve du consentement de l'annonceur; et

c) la mesure à partir de laquelle chacun des prix, frais et rémunérations est calculé.

Dans le cas où un annonceur ne consent pas au partage d'informations, le contrôleur d'accès fournit gratuitement à chaque éditeur des informations sur le prix moyen

quotidien payé par cet annonceur, y compris les déductions et suppléments éventuels, pour les publicités concernées.

Article 6

Obligations incombant aux contrôleurs d'accès susceptibles d'être précisées en vertu de l'article 8

1. Le contrôleurs d'accès se conforme à toutes les obligations énoncées au présent article pour chacun de ses services de plateforme essentiels énumérés dans la décision de désignation conformément à l'article 3, paragraphe 9.

2. 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.

Aux fins du premier alinéa, les données qui ne sont pas accessibles au public comprennent toutes les données agrégées et non agrégées générées par les entreprises utilisatrices qui peuvent être déduites ou collectées au travers des activités commerciales de ces entreprises ou de leurs clients, y compris les données concernant les clics, les recherches, les vues et la voix, dans le cadre des services de plateforme essentiels concernés ou de services fournis conjointement aux services de plateforme essentiels concernés du contrôleur d'accès, ou à leur appui.

3. Le contrôleur d'accès autorise et permet techniquement la désinstallation facile par les utilisateurs finaux de toute application logicielle dans son système d'exploitation, sans préjudice de la possibilité pour ce 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.

Le contrôleur d'accès autorise et permet techniquement la modification facile par les utilisateurs finaux des paramètres par défaut de son système d'exploitation, son assistant virtuel et son navigateur internet qui dirigent ou orientent les utilisateurs finaux vers des produits et des services proposés par le contrôleur d'accès. Pour ce faire, il invite notamment les utilisateurs finaux, au moment de leur première utilisation de son moteur de recherche en ligne, son assistant virtuel ou son navigateur internet énuméré dans la décision de désignation conformément à l'article 3, paragraphe 9, à choisir dans une liste des principaux fournisseurs de services disponibles, le moteur de recherche en ligne, assistant virtuel ou navigateur internet vers lequel le système d'exploitation du contrôleur d'accès dirige ou oriente les utilisateurs par défaut, et le moteur de recherche en ligne vers lequel l'assistant virtuel et le navigateur internet du contrôleur d'accès dirige ou oriente les utilisateurs par défaut.

4. Le contrôleur d'accès autorise et permet techniquement l'installation et l'utilisation effective d'applications logicielles ou de boutiques d'applications logicielles de tiers utilisant ou interopérant avec son système d'exploitation, et permet l'accès à ces applications logicielles ou boutiques d'applications logicielles par des moyens autres que les services de plateforme essentiels concernés du contrôleur d'accès. Le cas échéant, le contrôleur d'accès n'empêche pas une application logicielle ou boutique d'application

logicielle de tiers téléchargée d'inviter les utilisateurs finaux à choisir s'ils souhaitent utiliser par défaut ladite application logicielle ou boutique d'application logicielle téléchargée. Le contrôleur d'accès permet techniquement aux utilisateurs finaux qui choisissent d'utiliser par défaut ladite application logicielle ou boutique d'application logicielle téléchargée de procéder facilement à ce changement.

Rien n'empêche le contrôleur d'accès de prendre, dans la mesure où elles ne vont pas au-delà de ce qui est strictement nécessaire et proportionné, des mesures visant à 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, à condition que ces mesures soient dûment justifiées par le contrôleur d'accès.

En outre, rien n'empêche le contrôleur d'accès d'appliquer, dans la mesure où elles ne vont pas au-delà de ce qui est strictement nécessaire et proportionné, des mesures et des paramètres autres que les paramètres par défaut permettant aux utilisateurs finaux de protéger efficacement la sécurité en ce qui concerne les applications logicielles ou les boutiques d'applications logicielles de tiers, à condition que ces mesures et paramètres autres que les paramètres par défaut soient dûment justifiés par le contrôleur d'accès.

5. Le contrôleur d'accès n'accorde pas, en matière de classement ainsi que pour l'indexation et l'exploration qui y sont liées, un traitement plus favorable aux services et produits proposés par le contrôleur d'accès lui-même qu'aux services ou produits similaires d'un tiers. Le contrôleur d'accès applique des conditions transparentes, équitables et non discriminatoires à ce classement.

6. Le contrôleur d'accès ne restreint pas techniquement ou d'une autre manière la capacité des utilisateurs finaux de changer d'applications logicielles et de services qui sont accessibles en utilisant les services de plateforme essentiels du contrôleur d'accès et de s'y abonner, y compris en ce qui concerne le choix des services d'accès à l'internet pour les utilisateurs finaux.

7. Le contrôleur d'accès permet gratuitement aux fournisseurs de services et aux fournisseurs de matériel informatique d'interopérer efficacement avec les mêmes caractéristiques matérielles et logicielles auxquelles on accède ou qui sont contrôlées par l'intermédiaire du système d'exploitation ou de l'assistant virtuel énuméré dans la décision de désignation conformément à l'article 3, paragraphe 9, que celles qui sont disponibles pour les services ou le matériel fournis par le contrôleur d'accès, ainsi que d'accéder à ces caractéristiques aux fins de l'interopérabilité. En outre, le contrôleur d'accès permet gratuitement aux entreprises utilisatrices et à d'autres fournisseurs de services fournis conjointement à des services de plateforme essentiels, ou à l'appui de ceux-ci, d'interopérer effectivement avec les mêmes caractéristiques du système d'exploitation, matérielles ou logicielles, que ces caractéristiques fassent partie ou non d'un système d'exploitation, que celles qui sont disponibles pour ce contrôleur d'accès ou que celui-ci utilise dans le cadre de la fourniture de tels services, ainsi que d'accéder à ces caractéristiques aux fins de l'interopérabilité.

Rien n'empêche le contrôleur d'accès de prendre des mesures strictement nécessaires et proportionnées visant à éviter que l'interopérabilité ne compromette l'intégrité du système d'exploitation, de l'assistant virtuel, du matériel informatique ou du logiciel qu'il fournit, à condition que ces mesures soient dûment justifiées par le contrôleur d'accès.

8. Le contrôleur d'accès fournit aux annonceurs et aux éditeurs, ainsi qu'aux tiers autorisés par les annonceurs et les éditeurs, à leur demande et gratuitement, un accès aux

outils de mesure de performance du contrôleur d'accès et aux données qui leur sont nécessaires pour effectuer leur propre vérification indépendante de l'inventaire publicitaire, notamment les données agrégées et non agrégées. Ces données sont fournies de manière à permettre aux annonceurs et aux éditeurs d'utiliser leurs propres outils de vérification et de mesure afin d'évaluer la performance des services de plateforme essentiels fournis par le contrôleur d'accès.

9. Le contrôleur d'accès assure aux utilisateurs finaux et aux tiers autorisés par un utilisateur final, à leur demande et gratuitement, la portabilité effective des données fournies par l'utilisateur final ou générées par l'activité de l'utilisateur final dans le cadre de l'utilisation du service de plateforme essentiel concerné, y compris en fournissant gratuitement des outils facilitant l'exercice effectif de cette portabilité des données, et notamment en octroyant un accès continu et en temps réel à ces données.

10. Le contrôleur d'accès assure gratuitement aux entreprises utilisatrices et aux tiers autorisés par les entreprises utilisatrices, à leur demande, un accès et une utilisation effectifs, de haute qualité, continus et en temps réel en ce qui concerne les données agrégées et non agrégées, y compris les données à caractère personnel, fournies ou générées dans le cadre de l'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, par ces entreprises utilisatrices et par les utilisateurs finaux qui se servent des produits et services fournis par ces entreprises utilisatrices. En ce qui concerne les données à caractère personnel, le contrôleur d'accès ne donne un tel accès aux données à caractère personnel et ne les utilise que lorsque les données sont directement liées à l'utilisation faite par les utilisateurs finaux en lien avec les produits ou services que l'entreprise utilisatrice concernée fournit par l'intermédiaire du service de plateforme essentiel concerné, et lorsque les utilisateurs finaux optent pour un tel partage de données en donnant leur consentement.

11. Le contrôleur d'accès procure à toute entreprise tierce fournissant des moteurs de recherche en ligne, à sa demande et à des conditions équitables, raisonnables et non discriminatoires, un accès aux données concernant les classements, requêtes, clics et vues en lien avec les recherches gratuites et payantes générées par les utilisateurs finaux sur ses moteurs de recherche en ligne. Toutes ces données concernant les requêtes, clics et vues constituent des données à caractère personnel et sont anonymisées.

12. Le 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.

La Commission évalue si les conditions générales d'accès publiées sont conformes au présent paragraphe.

13. Le contrôleur d'accès ne dispose pas de conditions générales de résiliation de la fourniture d'un service de plateforme essentiel qui soient disproportionnées. Le contrôleur d'accès veille à ce que les conditions de résiliation puissent être appliquées sans difficulté excessive.

Article 7

Obligations incombant aux contrôleurs d'accès concernant l'interopérabilité des services de communications interpersonnelles non fondés sur la numérotation

1. Lorsqu'un contrôleur d'accès fournit des services de communications interpersonnelles non fondés sur la numérotation qui sont énumérés dans la décision de désignation conformément à l'article 3, paragraphe 9, il rend les fonctionnalités de base de ses services de communications interpersonnelles non fondés sur la numérotation interopérables avec les services de communications interpersonnelles non fondés sur la numérotation de tout autre fournisseur qui propose ou a l'intention de proposer de tels services dans l'Union, en fournissant sur demande et gratuitement les interfaces techniques nécessaires ou des solutions similaires qui facilitent l'interopérabilité.

2. Le contrôleur d'accès rend interopérables au moins les fonctionnalités de base visées au paragraphe 1 énumérées ci-après dès lors qu'il fournit lui-même ces fonctionnalités à ses propres utilisateurs finaux:

a) à la suite de l'établissement de la liste figurant dans la décision de désignation conformément à l'article 3, paragraphe 9:

i) messagerie textuelle de bout en bout entre deux utilisateurs finaux individuels;

ii) partage d'images, de messages vocaux, de vidéos et d'autres fichiers joints dans les communications de bout en bout entre deux utilisateurs finaux individuels;

b) dans un délai de deux ans à compter de la désignation:

i) messagerie textuelle de bout en bout entre des groupes d'utilisateurs finaux individuels;

ii)partage d'images, de messages vocaux, de vidéos et d'autres fichiers joints dans les communications de bout en bout entre une conversation de groupe et un utilisateur final individuel;

c) dans un délai de quatre ans à compter de la désignation:

i) appels vocaux de bout en bout entre deux utilisateurs finaux individuels;

ii)appels vidéo de bout en bout entre deux utilisateurs finaux individuels;

iii) appels vocaux de bout en bout entre une conversation de groupe et un utilisateur final individuel;

iv)appels vidéo de bout en bout entre une conversation de groupe et un utilisateur final individuel.

3. Le niveau de sécurité, y compris le chiffrement de bout en bout, le cas échéant, que le contrôleur d'accès fournit à ses propres utilisateurs finaux est maintenu dans l'ensemble des services interopérables.

4. Le contrôleur d'accès publie une offre de référence énonçant les détails techniques et les conditions générales d'interopérabilité avec ses services de communications interpersonnelles non fondés sur la numérotation, y compris les détails nécessaires concernant le niveau de sécurité et le chiffrement de bout en bout. Le contrôleur d'accès

publie cette offre de référence avant la fin de la période visée à l'article 3, paragraphe 10, et la met à jour si nécessaire.

5. À la suite de la publication de l'offre de référence conformément au paragraphe 4, tout fournisseur de services de communications interpersonnelles non fondés sur la numérotation qui propose ou a l'intention de proposer de tels services dans l'Union peut demander l'interopérabilité avec les services de communications interpersonnelles non fondés sur la numérotation fournis par le contrôleur d'accès. Une telle demande peut porter sur tout ou partie des fonctionnalités de base énumérées au paragraphe 2. Le contrôleur d'accès accepte toute demande raisonnable d'interopérabilité dans un délai de trois mois à compter de la réception de cette demande en rendant opérationnelles les fonctionnalités de base demandées.

6. La Commission peut, à titre exceptionnel et sur demande motivée du contrôleur d'accès, reporter les délais prévus pour se conformer au paragraphe 2 ou 5 lorsque le contrôleur d'accès démontre que cela est nécessaire pour assurer l'interopérabilité effective et maintenir le niveau de sécurité requis, y compris le chiffrement de bout en bout, le cas échéant.

7. Les utilisateurs finaux des services de communications interpersonnelles non fondés sur la numérotation du contrôleur d'accès et du fournisseur de services de communications interpersonnelles non fondés sur la numérotation qui formule la demande demeurent libres de décider s'ils utilisent les fonctionnalités de base interopérables qui peuvent être fournies par le contrôleur d'accès au titre du paragraphe 1.

8. Le contrôleur d'accès recueille et échange avec le fournisseur de services de communications interpersonnelles non fondés sur la numérotation qui formule une demande d'interopérabilité uniquement les données à caractère personnel d'utilisateurs finaux qui sont strictement nécessaires à la fourniture d'une interopérabilité effective. Toute collecte et tout échange de données à caractère personnel de ce type sont pleinement conformes au règlement (UE) 2016/679 et à la directive 2002/58/CE.

9. Rien n'empêche le contrôleur d'accès de prendre des mesures visant à éviter que les demandes d'interopérabilité formulées par des fournisseurs tiers de services de communications interpersonnelles non fondés sur la numérotation ne compromettent l'intégrité, la sécurité et la confidentialité de ses services, à condition que ces mesures soient strictement nécessaires et proportionnées, et soient dûment justifiées par le contrôleur d'accès.

Article 8

Respect des obligations incombant aux contrôleurs d'accès

1. Le contrôleur d'accès assure et démontre le respect des obligations prévues aux articles 5, 6 et 7 du présent règlement. Les mesures que le contrôleur d'accès met en œuvre pour garantir la conformité avec lesdits articles atteignent effectivement les objectifs du présent règlement et de l'obligation concernée. Le contrôleur d'accès veille à ce que la mise en œuvre de ces mesures respecte le droit applicable, en particulier le règlement (UE) 2016/679, la directive 2002/58/CE, la législation relative à la cybersécurité, à la protection des consommateurs et à la sécurité des produits, ainsi que les exigences en matière d'accessibilité.

2. La Commission peut, de sa propre initiative ou à la demande d'un contrôleur d'accès conformément au paragraphe 3 du présent article, ouvrir la procédure prévue à l'article 20.

La Commission peut adopter un acte d'exécution, qui précise les mesures que le contrôleur d'accès concerné est tenu de mettre en œuvre afin de se conformer effectivement aux obligations énoncées aux articles 6 et 7. Cet acte d'exécution est adopté dans les six mois suivant l'ouverture de la procédure prévue à l'article 20, en conformité avec la procédure consultative visée à l'article 50, paragraphe 2.

Lorsqu'elle ouvre la procédure de sa propre initiative, en cas de contournement, conformément à l'article 13, ces mesures peuvent porter sur les obligations énoncées aux articles 5, 6 et 7.

3. Un contrôleur d'accès peut demander à la Commission d'engager un processus afin de déterminer si les mesures que ce contrôleur d'accès entend mettre en œuvre ou a mises en œuvre pour se conformer aux articles 6 et 7 atteignent effectivement l'objectif de l'obligation pertinente dans la situation spécifique du contrôleur d'accès. La Commission dispose d'une marge d'appréciation pour décider s'il y a lieu d'engager un tel processus, dans le respect des principes d'égalité de traitement, de proportionnalité et de bonne administration.

Dans sa demande, le contrôleur d'accès fournit un mémoire motivé pour expliquer les mesures qu'il entend mettre en œuvre ou a mises en œuvre. Le contrôleur d'accès fournit en outre une version non confidentielle de son mémoire motivé qui peut être partagée avec des tiers conformément au paragraphe 6.

4. Les paragraphes 2 et 3 sont sans préjudice des pouvoirs conférés à la Commission en vertu des articles 29, 30 et 31.

5. En vue de l'adoption de la décision visée au paragraphe 2, la Commission fait part de ses constatations préliminaires au contrôleur d'accès dans un délai de trois mois à compter de l'ouverture de la procédure au titre de l'article 20. Dans ses constatations préliminaires, la Commission explique les mesures qu'elle envisage de prendre ou que le contrôleur d'accès concerné devrait prendre, selon elle, afin de donner suite de manière effective aux constatations préliminaires.

6. Afin de permettre effectivement aux tiers intéressés de présenter des observations, la Commission publie, lorsqu'elle communique ses constatations préliminaires au contrôleur d'accès conformément au paragraphe 5 ou le plus tôt possible après une telle communication, une synthèse non confidentielle de la situation et les mesures qu'elle envisage de prendre ou que le contrôleur d'accès concerné devrait prendre selon elle. La Commission fixe un délai raisonnable dans lequel ces observations peuvent être formulées.

7. En précisant les mesures visées au paragraphe 2, la Commission veille à ce qu'elles atteignent effectivement les objectifs du présent règlement et de l'obligation pertinente et à ce qu'elles soient proportionnées compte tenu de la situation spécifique du contrôleur d'accès et du service concerné.

8. Dans le but de préciser les obligations prévues à l'article 6, paragraphes 11 et 12, la Commission évalue en outre si les mesures envisagées ou mises en œuvre garantissent qu'aucun déséquilibre ne demeure entre les droits et les obligations des entreprises utilisatrices et si les mesures ne confèrent pas elles-mêmes au contrôleur d'accès un

avantage disproportionné par rapport au service qu'il fournit aux entreprises utilisatrices.

9. En ce qui concerne la procédure visée au paragraphe 2, la Commission peut, sur demande ou de sa propre initiative, décider de la rouvrir lorsque:

a) l'un des faits sur lesquels la décision repose subit un changement important; ou

b) la décision repose sur des informations incomplètes, inexactes ou dénaturées; ou

c) les mesures énoncées dans la décision ne sont pas efficaces.

Article 9

Suspension

1. Lorsque le contrôleur d'accès démontre dans une demande motivée que le respect d'une obligation spécifique énoncée à l'article 5, 6 ou 7 concernant un service de plateforme essentiel énuméré dans la décision de désignation conformément à l'article 3, paragraphe 9, menacerait, en raison de circonstances exceptionnelles échappant à son contrôle, la viabilité économique de ses activités dans l'Union, la Commission peut adopter un acte d'exécution établissant sa décision de suspendre, à titre exceptionnel, entièrement ou partiellement, l'obligation spécifique visée dans cette demande motivée (ci-après dénommée «décision de suspension»). Dans cet acte d'exécution, la Commission étaye sa décision de suspension en indiquant les circonstances exceptionnelles justifiant la suspension. La portée et la durée de cet acte d'exécution sont limitées à ce qui est nécessaire pour remédier à cette menace pour la viabilité du contrôleur d'accès. La Commission s'efforce d'adopter cet acte d'exécution sans tarder et au plus tard trois mois après réception d'une demande complète et motivée. Cet acte d'exécution est adopté en conformité avec la procédure consultative visée à l'article 50, paragraphe 2.

2. Lorsqu'une suspension est accordée en vertu du paragraphe 1, la Commission réexamine sa décision de suspension chaque année, à moins qu'un intervalle plus court ne soit indiqué dans ladite décision. À la suite de ce réexamen, la Commission lève entièrement ou partiellement la suspension, ou décide que les conditions visées au paragraphe 1 demeurent remplies.

3. En cas d'urgence, sur demande motivée d'un contrôleur d'accès, la Commission peut suspendre provisoirement l'application d'une obligation spécifique visée au paragraphe 1 pour un ou plusieurs services de plateforme essentiels spécifiques, avant même d'adopter la décision visée audit paragraphe. Une telle demande peut être présentée et acceptée à tout moment, dans l'attente de l'évaluation de la Commission en application du paragraphe 1.

4. Lors de l'évaluation de la demande visée aux paragraphes 1 et 3, la Commission tient compte en particulier de l'incidence du respect de l'obligation spécifique sur la viabilité économique des activités du contrôleur d'accès dans l'Union ainsi que sur les tiers, en particulier les PME et les consommateurs. La suspension peut être soumise à des conditions et obligations devant être définies par la Commission afin de garantir un juste équilibre entre ces intérêts et les objectifs du présent règlement.

Article 10

Exemption pour raisons de santé publique et de sécurité publique

1. Sur demande motivée d'un contrôleur d'accès ou de sa propre initiative, la Commission peut adopter un acte d'exécution établissant sa décision d'exempter ce contrôleur d'accès, entièrement ou partiellement, d'une obligation particulière prévue à l'article 5, 6 ou 7 en ce qui concerne un service de plateforme essentiel énuméré dans la décision de désignation conformément à l'article 3, paragraphe 9, lorsqu'une telle exemption est justifiée par les motifs énoncés au paragraphe 3 du présent article (ci-après dénommée «décision d'exemption»). La Commission adopte la décision d'exemption dans un délai de trois mois après réception d'une demande complète et motivée, et fournit une déclaration motivée expliquant les raisons de l'exemption. Cet acte d'exécution est adopté en conformité avec la procédure consultative visée à l'article 50, paragraphe 2.

2. Lorsqu'une exemption est accordée en vertu du paragraphe 1, la Commission réexamine sa décision d'exemption lorsque le motif de l'exemption n'existe plus ou au minimum chaque année. À la suite de ce réexamen, la Commission lève entièrement ou partiellement l'exemption ou décide que les conditions du paragraphe 1 demeurent remplies.

3. Une exemption en vertu du paragraphe 1 ne peut être accordée que pour des motifs de santé publique ou de sécurité publique.

4. En cas d'urgence, sur demande motivée d'un contrôleur d'accès ou de sa propre initiative, la Commission peut suspendre provisoirement l'application d'une obligation spécifique visée au paragraphe 1 pour un ou plusieurs services de plateforme essentiels spécifiques, avant même d'adopter la décision visée audit paragraphe. Une telle demande peut être présentée et acceptée à tout moment, dans l'attente de l'évaluation de la Commission en application du paragraphe 1.

5. Lors de l'évaluation de la demande visée aux paragraphes 1 et 4, la Commission tient compte en particulier de l'incidence du respect de l'obligation spécifique sur les motifs énumérés au paragraphe 3, ainsi que des effets sur le contrôleur d'accès concerné et sur les tiers. La Commission peut soumettre la suspension à des conditions et obligations afin de garantir un juste équilibre entre les objectifs visés par les motifs énoncés au paragraphe 3 et les objectifs du présent règlement.

Article 11

Établissement de rapports

1. Dans les six mois suivant sa désignation au titre de l'article 3, et conformément à l'article 3, paragraphe 10, le contrôleur d'accès remet à la Commission un rapport décrivant de manière détaillée et transparente les mesures qu'il a mises en œuvre pour garantir le respect des obligations énoncées aux articles 5, 6 et 7.

2. Dans le délai visé au paragraphe 1, le contrôleur d'accès publie et remet à la Commission une synthèse non confidentielle de ce rapport.

Le contrôleur d'accès met à jour au moins annuellement ce rapport et cette synthèse non confidentielle.

La Commission insère sur son site internet un lien vers cette synthèse non confidentielle.

Article 12

Mise à jour des obligations des contrôleurs d'accès

1. La Commission est habilitée à adopter des actes délégués conformément à l'article 49 pour compléter le présent règlement en ce qui concerne les obligations existantes énoncées aux articles 5 et 6. Ces actes délégués sont fondés sur une enquête de marché menée en vertu de l'article 19 qui a mis en évidence la nécessité de maintenir à jour ces obligations afin de lutter contre les pratiques qui limitent la contestabilité des services de plateforme essentiels ou qui sont déloyales au même titre que les pratiques qui sont l'objet des obligations énoncées aux articles 5 et 6.

2. Le champ d'application d'un acte délégué adopté conformément au paragraphe 1 se limite à:

a) élargir une obligation qui s'applique uniquement dans le cadre de certains services de plateforme essentiels à d'autres services de plateforme essentiels énumérés à l'article 2, point 2);

b) élargir une obligation dont bénéficient certaines entreprises utilisatrices ou utilisateurs finaux de manière à ce que d'autres entreprises utilisatrices ou utilisateurs finaux en soient bénéficiaires;

c) préciser les modalités d'exécution par les contrôleurs d'accès des obligations énoncées aux articles 5 et 6 afin de garantir le respect effectif de ces obligations;

d) élargir une obligation qui s'applique uniquement dans le cadre de certains services fournis conjointement à des services de plateforme essentiels, ou à leur appui, à d'autres services fournis conjointement à des services de plateforme essentiels, ou à leur appui;

e) élargir une obligation qui s'applique uniquement dans le cadre de certains types de données afin qu'elle s'applique à d'autres types de données;

f) ajouter des conditions supplémentaires lorsqu'une obligation impose certaines conditions concernant le comportement d'un contrôleur d'accès; ou

g) appliquer une obligation qui régit la relation entre plusieurs services de plateforme essentiels du contrôleur d'accès à la relation entre un service de plateforme essentiel et d'autres services du contrôleur d'accès.

3. La Commission est habilitée à adopter des actes délégués conformément à l'article 49 pour modifier le présent règlement en ce qui concerne la liste des fonctionnalités de base recensées à l'article 7, paragraphe 2, en ajoutant ou en supprimant des fonctionnalités de services de communications interpersonnelles non fondés sur la numérotation.

Ces actes délégués sont fondés sur une enquête de marché menée en vertu de l'article 19 qui a mis en évidence la nécessité de maintenir à jour ces obligations afin de lutter contre les pratiques qui limitent la contestabilité des services de plateforme essentiels ou qui sont déloyales au même titre que les pratiques qui sont l'objet des obligations énoncées à l'article 7.

4. La Commission est habilitée à adopter des actes délégués conformément à l'article 49 pour compléter le présent règlement en ce qui concerne les obligations prévues à l'article 7 en précisant les modalités d'exécution des obligations afin de garantir le respect effectif de ces obligations. Ces actes délégués sont fondés sur une enquête de marché menée en vertu de l'article 19 qui a mis en évidence la nécessité de maintenir à jour ces obligations afin de lutter contre les pratiques qui limitent la contestabilité des services de

plateforme essentiels ou qui sont déloyales au même titre que les pratiques qui sont l'objet des obligations énoncées à l'article 7.

5. Une pratique visée aux paragraphes 1, 3 et 4 est considérée comme limitant la contestabilité des services de plateforme essentiels ou comme déloyale:

a) lorsque cette pratique est le fait des contrôleurs d'accès et est susceptible d'entraver l'innovation et de limiter le choix pour les entreprises utilisatrices et les utilisateurs finaux parce qu'elle:

i) porte atteinte ou risque de porter atteinte durablement à la contestabilité d'un service de plateforme essentiel ou d'autres services dans le secteur numérique en raison de la création ou du renforcement d'obstacles empêchant d'autres entreprises de s'implanter ou de se développer en tant que fournisseurs d'un service de plateforme essentiel ou d'autres services dans le secteur numérique; ou

ii) empêche les autres opérateurs d'avoir le même accès que le contrôleur d'accès à un intrant clé; ou

b) lorsqu'il existe un déséquilibre entre les droits et les obligations des entreprises utilisatrices et que le contrôleur d'accès obtient un avantage des entreprises utilisatrices qui est disproportionné par rapport au service fourni par ce contrôleur d'accès à ces entreprises utilisatrices.

Article 13

Anticontournement

1. Une entreprise fournissant des services de plateforme essentiels ne segmente pas, ni ne divise, subdivise, fragmente ou fractionne ces services par des moyens contractuels, commerciaux, techniques ou autres dans le but de contourner les seuils quantitatifs fixés à l'article 3, paragraphe 2. Aucune de ces pratiques de la part d'une entreprise n'empêche la Commission de désigner celle-ci comme contrôleur d'accès au titre de l'article 3, paragraphe 4.

2. Lorsqu'elle soupçonne qu'une entreprise fournissant des services de plateforme essentiels met en œuvre une pratique visée au paragraphe 1, la Commission peut exiger de cette entreprise toute information qu'elle juge nécessaire pour déterminer si cette entreprise s'est livrée à une telle pratique.

3. Le contrôleur d'accès veille à ce que les obligations des articles 5, 6 et 7 soient pleinement et effectivement respectées.

4. Le contrôleur d'accès ne se livre à aucun comportement compromettant le respect effectif des obligations des articles 5, 6 et 7, que ce comportement soit de nature contractuelle, commerciale, technique ou autre, ou qu'il consiste en l'utilisation de techniques comportementales ou d'une conception d'interface.

5. Si le consentement est requis pour la collecte, le traitement, l'utilisation croisée et le partage de données à caractère personnel afin que le respect du présent règlement soit garanti, le contrôleur d'accès prend les mesures nécessaires, soit pour permettre aux

entreprises utilisatrices d'obtenir directement le consentement requis au traitement de ces données, lorsque ce consentement est exigé en application du règlement (UE) 2016/679 ou de la directive 2002/58/CE, soit pour se conformer aux règles et principes de l'Union en matière de protection des données et de la vie privée par d'autres moyens, dont la fourniture aux entreprises utilisatrices de données dûment anonymisées, s'il y a lieu. Le contrôleur d'accès ne rend pas l'obtention de ce consentement par les entreprises utilisatrices plus lourde que pour ses propres services.

6. Le contrôleur d'accès ne détériore ni les conditions, ni la qualité de l'un de ses services de plateforme essentiels fournis aux entreprises utilisatrices ou aux utilisateurs finaux qui font valoir leurs droits ou choix prévus aux articles 5, 6 et 7, et ne rend pas l'exercice de ces droits ou choix excessivement difficile, y compris en proposant des choix à l'utilisateur final de manière partiale, ou encore en utilisant la structure, la conception, la fonction ou le mode de fonctionnement d'une interface utilisateur ou d'une partie connexe pour perturber l'autonomie des utilisateurs finaux ou des entreprises utilisatrices, leur prise de décision ou leur libre choix.

7. Lorsque le contrôleur d'accès contourne ou tente de contourner l'une des obligations énoncées à l'article 5, 6 ou 7 d'une manière décrite aux paragraphes 4, 5 et 6 du présent article, la Commission peut ouvrir la procédure prévue à l'article 20 et adopter un acte d'exécution visé à l'article 8, paragraphe 2, afin de préciser les mesures que le contrôleur d'accès est tenu de mettre en œuvre.

8. Le paragraphe 6 du présent article est sans préjudice des pouvoirs conférés à la Commission en vertu des articles 29, 30 et 31.

Article 14

Obligation d'informer sur les concentrations

1. Le contrôleur d'accès informe la Commission de tout projet de concentration au sens de l'article 3 du règlement (CE) n° 139/2004, lorsque les entités qui fusionnent ou la cible de la concentration fournissent des services de plateforme essentiels ou tout autre service dans le secteur numérique ou permettent la collecte de données, que ce projet soit soumis à une obligation de notification à la Commission en application dudit règlement ou à une autorité nationale de concurrence compétente selon les règles nationales en matière de concentrations.

Le contrôleur d'accès informe la Commission de cette concentration avant sa réalisation et après la conclusion de l'accord, la publication de l'offre publique d'achat ou d'échange ou l'acquisition d'une participation de contrôle.

2. Les informations communiquées par le contrôleur d'accès conformément au paragraphe 1 renseignent au moins sur les entreprises concernées par la concentration, leurs chiffres d'affaires annuels mondiaux et au sein de l'Union, leurs domaines d'activité, y compris les activités directement liées à la concentration et la valeur transactionnelle de l'accord ou une estimation de celle-ci, et sont accompagnées d'un résumé relatif à la concentration, y compris sa nature et sa justification, et d'une liste des États membres concernés par la concentration.

Les informations communiquées par le contrôleur d'accès indiquent également, pour tous les services de plateforme essentiels concernés, leurs chiffres d'affaires annuels au sein de l'Union, le nombre d'entreprises utilisatrices actives par an et le nombre d'utilisateurs finaux actifs par mois, respectivement.

3. Si à la suite d'une concentration visée au paragraphe 1 du présent article, d'autres services de plateforme essentiels atteignent, individuellement, les seuils fixés à l'article 3, paragraphe 2, point b), le contrôleur d'accès concerné en informe la Commission dans les deux mois à compter de la réalisation de la concentration et fournit à la Commission les informations visées à l'article 3, paragraphe 2.

4. La Commission communique aux autorités compétentes des États membres toute information reçue en application du paragraphe 1 et publie chaque année la liste des acquisitions dont elle a été informée par les contrôleurs d'accès en application dudit paragraphe.

La Commission tient compte de l'intérêt légitime des entreprises à ce que leurs secrets d'affaires ne soient pas divulgués.

5. Les autorités compétentes des États membres peuvent utiliser les informations reçues au titre du paragraphe 1 du présent article pour demander à la Commission d'examiner la concentration conformément à l'article 22 du règlement (CE) n° 139/2004.

Article 15

Obligation d'audit

1. Dans les six mois suivant sa désignation conformément à l'article 3, le contrôleur d'accès soumet à la Commission une description ayant fait l'objet d'un audit indépendant de toutes les techniques de profilage des consommateurs qu'il applique dans le cadre de ses services de plateforme essentiels énumérés dans la décision de désignation conformément à l'article 3, paragraphe 9. La Commission transmet cette description ayant fait l'objet d'un audit au comité européen de la protection des données.

2. La Commission peut adopter un acte d'exécution visé à l'article 46, paragraphe 1, point g), afin de mettre au point la méthodologie et la procédure de l'audit.

3. Le contrôleur d'accès met à la disposition du public un aperçu de la description ayant fait l'objet d'un audit visée au paragraphe 1. Ce faisant, le contrôleur d'accès est autorisé à tenir compte de la nécessité que ses secrets d'affaires ne soient pas divulgués. Le contrôleur d'accès met à jour au moins annuellement cette description et cet aperçu.

CHAPITRE IV
ENQUÊTE DE MARCHÉ

Article 16

Ouverture d'une enquête de marché

1. Lorsque la Commission a l'intention de mener une enquête de marché en vue de l'adoption éventuelle de décisions en vertu des articles 17, 18 et 19, elle adopte une décision relative à l'ouverture d'une enquête de marché.

2. Nonobstant le paragraphe 1, la Commission peut exercer ses pouvoirs d'enquête en vertu du présent règlement avant d'ouvrir une enquête de marché conformément audit paragraphe.

3. La décision visée au paragraphe 1 précise:

a) la date d'ouverture de l'enquête de marché;

b) la description de la question sur laquelle porte l'enquête de marché;

c) le but de l'enquête de marché.

4. La Commission peut rouvrir une enquête de marché qu'elle a clôturée si:

a) l'un des faits sur lesquels repose une décision adoptée en vertu de l'article 17, 18 ou 19 subit un changement important; ou

b) la décision adoptée en vertu de l'article 17, 18 ou 19 repose sur des renseignements incomplets, inexacts ou dénaturés.

5. La Commission peut demander à une ou plusieurs autorités nationales compétentes de l'assister dans son enquête de marché.

Article 17

Enquête de marché pour la désignation des contrôleurs d'accès

1. La Commission peut mener une enquête de marché afin d'examiner si une entreprise fournissant des services de plateforme essentiels devrait être désignée comme étant un contrôleur d'accès en vertu de l'article 3, paragraphe 8, ou aux fins de déterminer les services de plateforme essentiels devant être recensés dans la décision de désignation en vertu de l'article 3, paragraphe 9. La Commission s'efforce de conclure son enquête de marché dans un délai de douze mois à compter de la date visée à l'article 16, paragraphe 3, point a). Afin de conclure son enquête de marché, la Commission adopte un acte d'exécution énonçant sa décision. Cet acte d'exécution est adopté en conformité avec la procédure consultative visée à l'article 50, paragraphe 2.

2. Au cours d'une enquête de marché menée en vertu du paragraphe 1 du présent article, la Commission s'efforce de communiquer ses constatations préliminaires à l'entreprise fournissant des services de plateforme essentiels concernée, dans un délai de six mois à compter de la date visée à l'article 16, paragraphe 3, point a). Dans ses constatations préliminaires, la Commission explique si elle estime, à titre provisoire, qu'il est approprié que ladite entreprise soit désignée comme contrôleur d'accès en vertu de l'article 3, paragraphe 8, et que les services de plateforme essentiels concernés soient énumérés conformément à l'article 3, paragraphe 9.

3. Lorsque l'entreprise fournissant des services de plateforme essentiels atteint les seuils fixés à l'article 3, paragraphe 2, mais qu'elle a présenté des arguments suffisamment étayés en vertu de l'article 3, paragraphe 5, qui ont manifestement remis en cause la présomption énoncée à l'article 3, paragraphe 2, la Commission s'efforce de conclure l'enquête de marché dans un délai de cinq mois à compter de la date visée à l'article 16, paragraphe 3, point a).

Dans un tel cas, la Commission s'efforce de communiquer à l'entreprise concernée ses constatations préliminaires conformément au paragraphe 2 du présent article dans un délai de trois mois à compter de la date visée à l'article 16, paragraphe 3, point a).

4. Lorsque la Commission, en vertu de l'article 3, paragraphe 8, désigne comme contrôleur d'accès une entreprise fournissant des services de plateforme essentiels qui ne jouit pas encore d'une position solide et durable dans ses activités, mais en jouira de manière prévisible dans un avenir proche, elle peut ne déclarer applicable à ce contrôleur d'accès qu'une ou plusieurs des obligations énoncées à l'article 5, paragraphes 3 à 6, et à

l'article 6, paragraphes 4, 7, 9, 10 et 13, telles qu'elles sont précisées dans la décision de désignation. La Commission ne déclare applicables que les obligations appropriées et nécessaires pour empêcher le contrôleur d'accès concerné d'acquérir, par des moyens déloyaux, une position solide et durable dans ses activités. La Commission réexamine cette désignation conformément à la procédure prévue à l'article 4.

Article 18

Enquête de marché portant sur un non-respect systématique

1. La Commission peut mener une enquête de marché afin d'examiner si un contrôleur d'accès a fait preuve d'un non-respect systématique. La Commission conclut cette enquête de marché dans un délai de douze mois à compter de la date visée à l'article 16, paragraphe 3, point a). Lorsqu'il ressort de l'enquête de marché qu'un contrôleur d'accès a systématiquement contrevenu à une ou plusieurs des obligations prévues à l'article 5, 6 ou 7 et qu'il a maintenu, renforcé ou étendu sa position de contrôleur d'accès au regard des caractéristiques énoncées à l'article 3, paragraphe 1, la Commission peut adopter un acte d'exécution imposant à un tel contrôleur d'accès toute mesure corrective comportementale ou structurelle qui soit proportionnée et nécessaire pour garantir le respect effectif du présent règlement. Cet acte d'exécution est adopté en conformité avec la procédure consultative visée à l'article 50, paragraphe 2.

2. La mesure corrective imposée conformément au paragraphe 1 du présent article peut inclure, dans la mesure où cette mesure corrective est proportionnée et nécessaire pour préserver ou rétablir l'équité et la contestabilité affectées par le non-respect systématique, l'interdiction faite au contrôleur d'accès, pendant une période limitée, de se lancer dans une concentration au sens de l'article 3 du règlement (CE) n° 139/2004 en ce qui concerne les services de plateforme essentiels ou d'autres services fournis dans le secteur numérique ou permettant la collecte de données, qui sont affectés par le non-respect systématique.

3. Un contrôleur d'accès est réputé avoir systématiquement contrevenu aux obligations prévues aux articles 5, 6 et 7 lorsque la Commission a émis au moins trois décisions constatant un manquement au titre de l'article 29 à l'encontre d'un contrôleur d'accès en ce qui concerne l'un de ses services de plateforme essentiels au cours d'une période de huit ans ayant précédé l'adoption de la décision d'ouverture d'une enquête de marché en vue de l'adoption éventuelle d'une décision selon le présent article.

4. La Commission communique ses constatations préliminaires au contrôleur d'accès concerné dans un délai de six mois à compter de la date visée à l'article 16, paragraphe 3, point a). Dans ses constatations préliminaires, la Commission explique si elle estime, à titre préliminaire, que les conditions prévues au paragraphe 1 du présent article sont réunies et quelle mesure ou quelles mesures correctives elle considère, à titre préliminaire, comme nécessaires et proportionnées.

5. Afin de permettre aux tiers intéressés de formuler effectivement des observations, la Commission publie, en même temps qu'elle communique ses constatations préliminaires au contrôleur d'accès conformément au paragraphe 4 ou le plus tôt possible après une telle communication, une synthèse non confidentielle de l'affaire et des mesures correctives qu'elle envisage d'imposer. La Commission fixe un délai raisonnable dans lequel de telles observations doivent être formulées.

6. Lorsque la Commission a l'intention d'adopter une décision en vertu du paragraphe 1 du présent article en rendant obligatoires les engagements que le contrôleur d'accès propose de prendre en vertu de l'article 25, elle publie une synthèse non confidentielle de l'affaire ainsi que l'essentiel du contenu des engagements. Les tiers intéressés peuvent soumettre leurs observations dans un délai raisonnable qui est fixé par la Commission.

7. Au cours de l'enquête de marché, la Commission peut en prolonger la durée, à condition que cette prolongation se justifie par des motifs objectifs et soit proportionnée. Cette prolongation peut s'appliquer au délai imparti à la Commission pour formuler ses constatations préliminaires ou au délai imparti pour l'adoption de la décision finale. La durée totale de la ou des prolongations décidées en vertu du présent paragraphe ne dépasse pas six mois.

8. Afin de garantir le respect effectif des obligations prévues aux articles 5, 6 et 7 par le contrôleur d'accès, la Commission réexamine régulièrement les mesures correctives qu'elle impose conformément aux paragraphes 1 et 2 du présent article. La Commission est habilitée à modifier ces mesures correctives si, après une nouvelle enquête de marché, elle estime que celles-ci ne sont pas efficaces.

Article 19

Enquête de marché portant sur les nouveaux services et les nouvelles pratiques

1. La Commission peut mener une enquête de marché afin d'examiner s'il conviendrait d'inscrire un ou plusieurs services du secteur numérique sur la liste des services de plateforme essentiels prévus à l'article 2, point 2), ou afin de détecter des pratiques qui limitent la contestabilité des services de plateforme essentiels ou qui sont déloyaux et auxquels le présent règlement ne permet pas de remédier de manière effective. Dans son évaluation, la Commission tient compte de toutes les conclusions pertinentes des procédures au titre des articles 101 et 102 du traité sur le fonctionnement de l'Union européenne concernant les marchés numériques, ainsi que de toute autre évolution pertinente.

2. La Commission peut, lorsqu'elle mène une enquête de marché en vertu du paragraphe 1, consulter des tiers, y compris des entreprises utilisatrices et des utilisateurs finaux de services du secteur numérique qui font l'objet d'une enquête, ainsi que des entreprises utilisatrices et des utilisateurs finaux soumis à des pratiques faisant l'objet d'une enquête.

3. La Commission publie ses constatations dans un rapport dans un délai de dix-huit mois à compter de la date visée à l'article 16, paragraphe 3, point a).

Ce rapport est présenté au Parlement européen et au Conseil tout en étant, s'il y a lieu, assorti:

a) d'une proposition législative modifiant le présent règlement dans le but d'inclure des services supplémentaires du secteur numérique dans la liste des services de plateforme essentiels établie à l'article 2, point 2), ou d'intégrer de nouvelles obligations au chapitre III; ou

b) d'un projet d'acte délégué complétant le présent règlement en ce qui concerne les obligations énoncées aux articles 5 et 6, ou d'un projet d'acte délégué modifiant ou complétant le présent règlement en ce qui concerne les obligations énoncées à l'article 7, comme prévu à l'article 12.

Le cas échéant, la proposition législative modifiant le présent règlement visé au deuxième alinéa, point a), peut également viser à supprimer les services existants de la liste des services de plateforme essentiels établie à l'article 2, point 2), ou à supprimer des obligations existantes de l'article 5, 6 ou 7.

CHAPITRE V
POUVOIRS D'ENQUÊTE, DE COERCITION ET DE CONTRÔLE

Article 20

Ouverture d'une procédure

1. Lorsque la Commission a l'intention d'ouvrir une procédure en vue de l'adoption éventuelle de décisions au titre des articles 8, 29 et 30, elle adopte une décision relative à l'ouverture d'une procédure.

2. Nonobstant le paragraphe 1, la Commission peut exercer ses pouvoirs d'enquête en vertu du présent règlement avant d'ouvrir une procédure conformément audit paragraphe.

Article 21

Demandes de renseignements

1. Pour l'accomplissement de ses tâches au titre du présent règlement, la Commission peut, par simple demande ou par voie de décision, exiger des entreprises et associations d'entreprises qu'elles fournissent tous les renseignements nécessaires. La Commission peut également, par simple demande ou par voie de décision, exiger l'accès à toutes les données et algorithmes des entreprises et à des renseignements concernant les essais, ainsi que demander des explications les concernant.

2. Lorsqu'elle envoie une simple demande de renseignements à une entreprise ou à une association d'entreprises, la Commission indique la base juridique et le but de la demande, précise les renseignements demandés et fixe le délai dans lequel ils doivent être fournis, ainsi que les amendes prévues à l'article 30 qui est d'application au cas où des renseignements ou des explications incomplets, inexacts ou dénaturés seraient fournis.

3. Lorsque la Commission demande, par décision, aux entreprises et associations d'entreprises de fournir des renseignements, elle indique la base juridique et le but de la demande, précise les renseignements demandés et fixe le délai dans lequel les renseignements doivent être fournis. Lorsque la Commission demande aux entreprises de donner accès à toutes les données, tous les algorithmes et à des renseignements concernant les essais, elle indique le but de la demande et fixe le délai dans lequel il doit être accordé. Elle énonce également les amendes prévues à l'article 30 et indique ou inflige les astreintes prévues à l'article 31. De plus, elle informe du droit de faire examiner la décision par la Cour de justice.

4. Les entreprises ou associations d'entreprises ou leurs représentants fournissent les renseignements demandés, au nom de l'entreprise ou de l'association d'entreprises concernées. Les avocats dûment mandatés peuvent fournir les renseignements demandés au nom de leurs mandants. Ces derniers restent pleinement responsables du caractère complet, exact et non dénaturé des renseignements fournis.

5. À la demande de la Commission, les autorités compétentes des États membres fournissent à la Commission tous les renseignements en leur possession qui sont nécessaires à l'accomplissement des tâches qui lui sont assignées par le présent règlement.

Article 22

Pouvoir de mener des auditions et de recueillir des déclarations

1. Pour l'accomplissement de ses tâches au titre du présent règlement, la Commission peut entendre toute personne physique ou morale qui accepte d'être auditionnée, aux fins de la collecte d'informations, en lien avec l'objet d'une enquête. La Commission a le droit d'enregistrer ces auditions par tout moyen technique.

2. Lorsqu'une audition au titre du paragraphe 1 du présent article est menée dans les locaux d'une entreprise, la Commission en informe l'autorité nationale compétente de l'État membre chargée de faire appliquer les règles visées à l'article 1er, paragraphe 6, et sur le territoire duquel l'audition a lieu. Si cette autorité le demande, les agents de celle-ci peuvent prêter assistance aux agents et aux autres personnes les accompagnant mandatés par la Commission pour conduire l'audition.

Article 23

Pouvoirs d'effectuer des inspections

1. Pour l'accomplissement de ses tâches au titre du présent règlement, la Commission peut procéder à toutes les inspections nécessaires d'une entreprise ou d'une association d'entreprises.

2. Les agents et les autres personnes les accompagnant mandatés par la Commission pour procéder à une inspection sont investis des pouvoirs suivants :

a) **accéder** à tous les locaux, terrains et moyens de transport des entreprises et associations d'entreprises ;

b) **contrôler** les livres et autres documents en rapport avec l'activité, quel qu'en soit le support ;

c) **prendre ou obtenir** sous quelque forme que ce soit copie ou extrait des livres et documents ;

d) **exiger** de l'entreprise ou de l'association d'entreprises qu'elle donne accès à son organisation, son fonctionnement, son système informatique, ses algorithmes, son traitement des données et ses pratiques commerciales et qu'elle fournisse des explications sur ces différents éléments, et enregistrer ou consigner les explications données par tout moyen technique ;

e) **apposer** des scellés sur tous les locaux commerciaux et livres ou documents pendant la durée de l'inspection et dans la mesure où cela est nécessaire aux fins de celle-ci ;

f) **demande**r à tout représentant ou membre du personnel de l'entreprise ou de l'association d'entreprises des explications sur des faits ou documents en rapport avec l'objet et le but de l'inspection et enregistrer ses réponses par tout moyen technique.

3. Pour effectuer les inspections, la Commission peut demander le concours d'auditeurs ou d'experts nommés par la Commission en vertu de l'article 26, paragraphe 2, ainsi que celui de l'autorité nationale compétente de l'État membre chargée de faire appliquer les règles visées à l'article 1er, paragraphe 6, sur le territoire duquel l'inspection doit être menée.

4. Au cours des inspections, la Commission, les auditeurs ou experts nommés par cette dernière et l'autorité nationale compétente de l'État membre chargée de faire appliquer les règles visées à l'article 1er, paragraphe 6, sur le territoire duquel l'inspection doit être menée peuvent exiger de l'entreprise ou de l'association d'entreprises qu'elle donne accès à son organisation, son fonctionnement, son système informatique, ses algorithmes, son traitement des données et ses pratiques commerciales et qu'elle fournisse des explications sur ces différents éléments. La Commission et les auditeurs ou experts nommés par celle-ci et l'autorité nationale compétente de l'État membre chargée de faire appliquer les règles visées à l'article 1er, paragraphe 6, sur le territoire duquel l'inspection doit être menée peuvent poser des questions à tout représentant ou membre du personnel.

5. Les agents et les autres personnes les accompagnant mandatés par la Commission pour procéder à une inspection exercent leurs pouvoirs sur production d'un mandat écrit qui indique l'objet et le but de l'inspection, ainsi que les amendes prévues à l'article 30, qui s'appliquent au cas où les livres ou autres documents professionnels qui sont requis seraient présentés de manière incomplète et où les réponses aux demandes faites en application des paragraphes 2 et 4 du présent article seraient inexactes ou dénaturées. La Commission avise, en temps utile avant l'inspection, l'autorité nationale compétente de l'État membre chargée de faire appliquer les règles visées à l'article 1, paragraphe 6, sur le territoire duquel l'inspection doit être effectuée.

6. Les entreprises ou associations d'entreprises sont tenues de se soumettre à une inspection ordonnée par une décision de la Commission. Cette décision indique l'objet et le but de l'inspection, fixe la date à laquelle elle commence, indique les amendes et astreintes prévues aux articles 30 et 31 respectivement et informe du droit de faire examiner ladite décision devant la Cour de justice.

7. Les agents de l'autorité nationale compétente de l'État membre chargée de faire appliquer les règles visées à l'article 1er, paragraphe 6, sur le territoire duquel l'inspection doit être menée et les personnes mandatées ou nommées par cette autorité prêtent, à la demande de ladite autorité ou de la Commission, un concours actif aux agents et aux autres personnes les accompagnant mandatés par la Commission. Ils disposent à cette fin des pouvoirs prévus aux paragraphes 2 et 4 du présent article.

8. Lorsque les agents ou les autres personnes les accompagnant mandatés par la Commission constatent qu'une entreprise ou une association d'entreprises s'oppose à une inspection ordonnée en vertu du présent article, l'État membre concerné leur prête l'assistance nécessaire, en requérant au besoin la force publique ou une autorité disposant d'un pouvoir de contrainte équivalent, pour leur permettre d'exécuter leur mission d'inspection.

9. Si, en vertu du droit national, l'assistance prévue au paragraphe 8 du présent article requiert l'autorisation d'une autorité judiciaire, la Commission, l'autorité nationale compétente de l'État membre chargée de faire appliquer les règles visées à l'article 1er, paragraphe 6, ou les agents mandatés par ces autorités la sollicitent. Cette autorisation peut également être sollicitée par mesure de précaution.

10. Lorsqu'une autorisation visée au paragraphe 9 du présent article est sollicitée, l'autorité judiciaire nationale vérifie que la décision de la Commission est authentique et que les mesures coercitives envisagées ne sont ni arbitraires ni excessives par rapport à l'objet de l'inspection. Lorsqu'elle contrôle la proportionnalité des mesures coercitives, l'autorité judiciaire nationale peut demander à la Commission, directement ou par l'intermédiaire de l'autorité nationale compétente de l'État membre chargée de faire appliquer les règles visées à l'article 1er, paragraphe 6, des explications détaillées, notamment sur les motifs qui incitent la Commission à suspecter une infraction au présent règlement, ainsi que sur la gravité de l'infraction suspectée et sur la nature de l'implication de l'entreprise concernée. Cependant, l'autorité judiciaire nationale ne peut ni remettre en cause la nécessité de l'inspection ni exiger la communication des informations figurant dans le dossier de la Commission. Le contrôle de la légalité de la décision de la Commission est réservé à la Cour de justice.

Article 24

Mesures provisoires

En cas d'urgence justifiée par le fait qu'un préjudice grave et irréparable risque d'être causé aux entreprises utilisatrices ou aux utilisateurs finaux des contrôleurs d'accès, la Commission peut adopter un acte d'exécution ordonnant des mesures provisoires à l'encontre d'un contrôleur d'accès sur la base d'un constat prima facie d'infraction à l'article 5, 6 ou 7. Cet acte d'exécution est uniquement adopté dans le cadre d'une procédure ouverte en vue de l'adoption éventuelle d'une décision constatant un non-respect en application de l'article 29, paragraphe 1. Il est uniquement applicable pour une durée déterminée et est renouvelable dans la mesure où cela est nécessaire et opportun. Cet acte d'exécution est adopté en conformité avec la procédure consultative visée à l'article 50, paragraphe 2.

Article 25

Engagements

1. Si, au cours d'une procédure prévue par l'article 18, le contrôleur d'accès concerné propose de prendre des engagements pour les services de plateforme essentiels en cause afin de garantir le respect des obligations énoncées aux articles 5, 6 et 7, la Commission peut adopter un acte d'exécution rendant ces engagements obligatoires pour ce contrôleur d'accès et déclarer qu'il n'y a plus lieu d'agir. Cet acte d'exécution est adopté en conformité avec la procédure consultative visée à l'article 50, paragraphe 2.

2. La Commission peut, sur demande ou de sa propre initiative, rouvrir la procédure concernée par voie de décision lorsque :

a) l'un des faits sur lesquels la décision repose subit un changement important ;

b) le contrôleur d'accès concerné contrevient à ses engagements ;

c) la décision repose sur des informations incomplètes, inexactes ou dénaturées fournies par les parties ;

d) les engagements ne sont pas effectifs.

3. Si la Commission devait estimer que les engagements proposés par le contrôleur d'accès concerné ne peuvent pas garantir le respect effectif des obligations prévues aux

articles 5, 6 et 7, elle explique les raisons pour lesquelles elle ne rend pas ces engagements obligatoires dans la décision concluant la procédure en question.

Article 26

Contrôle des obligations et mesures

1. La Commission prend les mesures nécessaires pour contrôler la mise en œuvre et le respect effectifs des obligations prévues aux articles 5, 6 et 7 et des décisions prises en vertu des articles 8, 18, 24, 25 et 29. Ces mesures peuvent notamment consister à imposer au contrôleur d'accès l'obligation de conserver tous les documents jugés pertinents pour évaluer la mise en œuvre et le respect de ces obligations et décisions.

2. Les mesures visées au paragraphe 1 peuvent comprendre la nomination d'experts et d'auditeurs externes indépendants, ainsi que la désignation d'agents par les autorités nationales compétentes des États membres, pour aider la Commission à contrôler les obligations et mesures et lui apporter une expertise et des connaissances spécifiques.

Article 27

Renseignements en provenance de tiers

1. Tous les tiers, y compris les entreprises utilisatrices, les concurrents ou les utilisateurs finaux des services de plateforme essentiels énumérés dans la décision de désignation en vertu de l'article 3, paragraphe 9, ainsi que leurs représentants, peuvent informer l'autorité nationale compétente de l'État membre, chargée de faire appliquer les règles visées à l'article 1er, paragraphe 6, ou directement la Commission concernant toute pratique ou tout comportement des contrôleurs d'accès relevant du champ d'application du présent règlement.

2. L'autorité nationale compétente de l'État membre, chargée de faire appliquer les règles visées à l'article 1er, paragraphe 6, et la Commission ont toute latitude en ce qui concerne les mesures appropriées et ne sont pas tenues de donner suite aux renseignements reçus.

3. Lorsque l'autorité nationale compétente de l'État membre, chargée de faire appliquer les règles visées à l'article 1er, paragraphe 6, détermine, sur la base des renseignements reçus en vertu du paragraphe 1 du présent article, qu'il peut y avoir un cas de non-respect du présent règlement, elle transmet ces renseignements à la Commission.

Article 28

Fonction de vérification de la conformité

1. Les contrôleurs d'accès mettent en place une fonction de vérification de la conformité, qui est indépendante des fonctions opérationnelles du contrôleur d'accès et fait appel à un ou plusieurs responsables de la conformité, y compris le responsable général de la fonction de vérification de la conformité.

2. Le contrôleur d'accès veille à ce que la fonction de vérification de la conformité visée au paragraphe 1 dispose d'une autorité, d'une stature et de ressources suffisantes, ainsi que d'un accès à l'organe de direction du contrôleur d'accès pour contrôler le respect du présent règlement par ce dernier.

3. L'organe de direction du contrôleur d'accès s'assure que les responsables de la conformité désignés conformément au paragraphe 1 disposent des qualifications professionnelles, des connaissances, de l'expérience et des aptitudes nécessaires pour mener à bien les tâches visées au paragraphe 5.

L'organe de direction du contrôleur d'accès veille également à ce que le responsable général de la fonction de vérification de la conformité soit un cadre supérieur ayant une responsabilité distincte pour la fonction de vérification de la conformité.

4. Le responsable général de la fonction de vérification de la conformité fait directement rapport à l'organe de direction du contrôleur d'accès et peut soulever des préoccupations et avertir cet organe en cas de risque de non-respect du présent règlement, sans préjudice des responsabilités de l'organe de direction dans ses fonctions de surveillance et de gestion.

Il ne peut être congédié sans l'accord préalable de l'organe de direction du contrôleur d'accès.

5. Les responsables de la conformité désignés par le contrôleur d'accès en vertu du paragraphe 1 sont chargés des tâches suivantes:

a) organiser, suivre et contrôler les mesures et activités des contrôleurs d'accès visant à assurer le respect du présent règlement;

b) informer et conseiller la direction et les employés du contrôleur d'accès en ce qui concerne le respect du présent règlement;

c) contrôler, le cas échéant, le respect des engagements rendus contraignants en vertu de l'article 25, sans préjudice de la possibilité pour la Commission de désigner des experts externes indépendants conformément à l'article 26, paragraphe 2;

d) coopérer avec la Commission aux fins du présent règlement.

6. Les contrôleurs d'accès communiquent à la Commission le nom et les coordonnées du responsable général de la fonction de vérification de la conformité.

7. L'organe de direction du contrôleur d'accès définit, supervise et rend compte de la mise en œuvre des dispositifs de gouvernance du contrôleur d'accès qui garantissent l'indépendance de la fonction de vérification de la conformité, y compris la répartition des responsabilités dans l'organisation du contrôleur d'accès et la prévention des conflits d'intérêts.

8. L'organe de direction approuve et réexamine périodiquement, au moins une fois par an, les stratégies et les politiques relatives à la prise en compte, à la gestion et au suivi du respect du présent règlement.

9. L'organe de direction consacre suffisamment de temps à la gestion et au suivi du respect du présent règlement. Il participe activement aux décisions relatives à la gestion et à l'exécution du présent règlement et veille à ce que des ressources suffisantes soient allouées en la matière.

Article 29

Non-respect

1. La Commission adopte un acte d'exécution établissant son constat de non-respect (ci-après dénommé «décision constatant un non-respect») lorsqu'elle constate qu'un contrôleur d'accès ne respecte pas un ou plusieurs des éléments suivants:

a) l'une des obligations prévues à l'article 5, 6 ou 7;

b) les mesures précisées par la Commission dans une décision adoptée en vertu de l'article 8, paragraphe 2;

c) les mesures correctives imposées en vertu de l'article 18, paragraphe 1;

d) les mesures provisoires ordonnées en vertu de l'article 24; ou

e) les engagements rendus juridiquement obligatoires en vertu de l'article 25.

Cet acte d'exécution est adopté en conformité avec la procédure consultative visée à l'article 50, paragraphe 2.

2. La Commission s'efforce d'adopter sa décision constatant un non-respect dans les douze mois suivant l'ouverture de la procédure prévue à l'article 20.

3. Avant d'adopter la décision constatant un non-respect, la Commission fait part de ses constatations préliminaires au contrôleur d'accès concerné. Dans ces constatations préliminaires, la Commission explique les mesures qu'elle envisage de prendre ou que le contrôleur d'accès devrait prendre, selon elle, afin de donner suite de manière effective aux constatations préliminaires.

4. Lorsqu'elle prévoit d'adopter une décision constatant un non-respect, la Commission peut consulter des tiers.

5. Dans la décision constatant un non-respect, la Commission ordonne au contrôleur d'accès de mettre fin au non-respect dans un délai approprié et de fournir des explications sur la manière dont il envisage de se mettre en conformité avec cette décision.

6. Le contrôleur d'accès fournit à la Commission la description des mesures qu'il a prises pour garantir le respect de la décision constatant un non-respect.

7. Lorsque la Commission décide de ne pas adopter une décision constatant un non-respect, elle clôt la procédure par voie de décision.

Article 30

Amendes

1. Dans la décision constatant un non-respect, la Commission peut infliger à un contrôleur d'accès des amendes jusqu'à concurrence de 10 % de son chiffre d'affaires total réalisé au niveau mondial au cours de l'exercice précédent lorsqu'elle constate que le contrôleur d'accès, volontairement ou par négligence, ne respecte pas:

a) l'une des obligations prévues aux articles 5, 6 et 7;

b) les mesures précisées par la Commission dans une décision adoptée en vertu de l'article 8, paragraphe 2;

c) les mesures correctives imposées en vertu de l'article 18, paragraphe 1;

d) les mesures provisoires ordonnées en vertu de l'article 24; ou

e) les engagements rendus juridiquement obligatoires en vertu de l'article 25.

2. Nonobstant le paragraphe 1 du présent article, dans une décision constatant un non-respect, la Commission peut infliger à un contrôleur d'accès des amendes allant jusqu'à 20 % de son chiffre d'affaires total réalisé au niveau mondial au cours de l'exercice précédent lorsqu'elle constate qu'un contrôleur d'accès a commis la même infraction à une obligation prévue à l'article 5, 6 ou 7, ou une infraction similaire, en ce qui concerne le même service de plateforme essentiel que celui pour lequel une infraction avait été constatée dans une décision constatant un non-respect adoptée au cours des huit années précédentes.

3. La Commission peut adopter une décision infligeant aux entreprises, y compris aux contrôleurs d'accès le cas échéant, et aux associations d'entreprises, des amendes jusqu'à concurrence de 1 % de leur chiffre d'affaires total réalisé au niveau mondial au cours de l'exercice précédent lorsque, volontairement ou par négligence, elles:

a) ne fournissent pas, dans le délai imparti, les renseignements requis pour l'appréciation de leur désignation comme contrôleurs d'accès en vertu de l'article 3 ou fournissent des renseignements inexacts, incomplets ou dénaturés;

b) ne respectent pas l'obligation d'information de la Commission prévue à l'article 3, paragraphe 3;

c) ne communiquent pas les renseignements exigés conformément à l'article 14, ou fournissent des renseignements inexacts, incomplets ou dénaturés;

d) ne présentent pas la description exigée au titre de l'article 15 ou fournissent des renseignements inexacts, incomplets ou dénaturés;

e) ne donnent pas l'accès aux données et algorithmes ou aux renseignements concernant les essais en réponse à une demande faite en vertu de l'article 21, paragraphe 3;

f) ne fournissent pas les renseignements exigés dans le délai fixé en vertu de l'article 21, paragraphe 3, ou fournissent des renseignements ou des explications, qui sont exigés en vertu de l'article 21 ou fournis lors d'une audition en vertu de l'article 22, inexacts, incomplets ou dénaturés;

g) omettent de rectifier, dans le délai fixé par la Commission, les renseignements inexacts, incomplets ou dénaturés donnés par un représentant ou un membre du personnel, ou omettent ou refusent de fournir des renseignements complets sur des faits en rapport avec l'objet et le but d'une inspection décidée en vertu de l'article 23;

h) refusent de se soumettre à une inspection décidée en vertu de l'article 23;

i) ne se conforment pas aux obligations imposées par la Commission en vertu de l'article 26; ou

j) n'introduisent pas une fonction de vérification de la conformité conformément à l'article 28; ou

k) ne respectent pas les conditions d'accès au dossier de la Commission conformément à l'article 34, paragraphe 4.

4. Pour déterminer le montant d'une amende, la Commission tient compte de la gravité, de la durée et de la récurrence ainsi que, pour les amendes infligées au titre du paragraphe 3, du retard causé à la procédure.

5. Lorsqu'une amende est infligée à une association d'entreprises en tenant compte du chiffre d'affaires de ses membres réalisé au niveau mondial et que cette association n'est pas solvable, cette dernière est tenue de lancer à ses membres un appel à contributions pour couvrir le montant de l'amende.

Si ces contributions n'ont pas été versées à l'association d'entreprises dans un délai fixé par la Commission, celle-ci peut exiger le paiement de l'amende directement par toute entreprise dont les représentants étaient membres des organes décisionnels concernés de ladite association.

Après avoir exigé le paiement conformément au deuxième alinéa, la Commission peut, lorsque cela est nécessaire pour garantir le paiement intégral de l'amende, exiger le paiement du solde par l'un quelconque des membres de l'association d'entreprises.

Cependant, la Commission n'exige pas le paiement visé au deuxième ou au troisième alinéa auprès des entreprises qui démontrent qu'elles n'ont pas appliqué la décision de l'association d'entreprises qui enfreignait le présent règlement et que soit elles en ignoraient l'existence, soit elles s'en étaient activement désolidarisées avant que la Commission n'ouvre une procédure en vertu de l'article 20.

La responsabilité financière de chaque entreprise en ce qui concerne le paiement de l'amende ne peut excéder 20 % de son chiffre d'affaires total réalisé au niveau mondial au cours de l'exercice précédent.

Article 31

Astreintes

1. La Commission peut adopter une décision infligeant aux entreprises, y compris aux contrôleurs d'accès s'il y a lieu, et aux associations d'entreprises des astreintes jusqu'à concurrence de 5 % du chiffre d'affaires journalier moyen réalisé au niveau mondial au cours de l'exercice précédent par jour, à compter de la date qu'elle fixe dans sa décision, pour les contraindre:

a) à respecter les mesures précisées par la Commission dans une décision adoptée en vertu de l'article 8, paragraphe 2;

b) à respecter la décision prise en vertu de l'article 18, paragraphe 1;

c) à fournir des renseignements exacts et complets dans le délai requis par une demande de renseignements formulée par voie de décision en vertu de l'article 21;

d) à garantir l'accès aux données, algorithmes et renseignements concernant les essais en réponse à une demande faite en vertu de l'article 21, paragraphe 3, et à fournir des explications les concernant, tel qu'exigé par une décision prise en vertu de l'article 21;

e) à se soumettre à une inspection ordonnée par voie de décision prise en vertu de l'article 23;

f) à respecter une décision ordonnant des mesures provisoires prises en vertu de l'article 24;

g) à respecter des engagements rendus juridiquement obligatoires par décision en vertu de l'article 25, paragraphe 1;

h) à respecter une décision prise en application de l'article 29, paragraphe 1.

2. Lorsque les entreprises, ou associations d'entreprises, ont satisfait à l'obligation pour l'exécution de laquelle l'astreinte a été infligée, la Commission peut adopter un acte d'exécution fixant le montant définitif de l'astreinte à un chiffre inférieur à celui qui résulte de la décision initiale. Cet acte d'exécution est adopté en conformité avec la procédure consultative visée à l'article 50, paragraphe 2.

Article 32

Prescription en matière d'imposition de sanctions

1. Les pouvoirs conférés à la Commission en vertu des articles 30 et 31 sont soumis à un délai de prescription de cinq ans.

2. La prescription court à compter du jour où l'infraction a été commise. Toutefois, pour les infractions continues ou répétées, la prescription ne court qu'à compter du jour où l'infraction a pris fin.

3. La prescription en matière d'imposition d'amendes ou d'astreintes est interrompue par tout acte de la Commission visant à mener une enquête sur le marché ou à poursuivre l'infraction. L'interruption de la prescription prend effet le jour où l'acte est notifié à au moins une entreprise ou association d'entreprises ayant participé à l'infraction. Constituent notamment des actes interrompant la prescription:

a) les demandes de renseignements de la Commission;

b) les autorisations écrites d'effectuer des inspections délivrées par la Commission à ses agents;

c)l'ouverture d'une procédure par la Commission en application de l'article 20.

4. La prescription court à nouveau à partir de chaque interruption. Toutefois, la prescription est acquise au plus tard le jour où un délai égal au double du délai de prescription arrive à expiration sans que la Commission ait prononcé une amende ou astreinte. Ce délai est prolongé de la période pendant laquelle la prescription est suspendue conformément au paragraphe 5.

5. La prescription en matière d'imposition d'amendes ou d'astreintes est suspendue aussi longtemps que la décision de la Commission fait l'objet d'une procédure pendante devant la Cour de justice.

Article 33

Prescription en matière d'exécution des sanctions

1. Le pouvoir de la Commission d'exécuter les décisions prises en vertu des articles 30 et 31 est soumis à un délai de prescription de cinq ans.

2. La prescription court à compter du jour où la décision est devenue définitive.

3. La prescription en matière d'exécution des sanctions est interrompue:

a) par la notification d'une décision modifiant le montant initial de l'amende ou de l'astreinte ou rejetant une demande tendant à obtenir une telle modification; ou

b) par tout acte de la Commission ou d'un État membre, agissant à la demande de la Commission, visant au recouvrement forcé de l'amende ou de l'astreinte.

4. La prescription court à nouveau à partir de chaque interruption.

5. La prescription en matière d'exécution des sanctions est suspendue:

a) aussi longtemps qu'un délai de paiement est accordé; ou

b) aussi longtemps que l'exécution forcée du paiement est suspendue en vertu d'une décision de la Cour de justice ou d'une décision d'une juridiction nationale.

Article 34

Droit d'être entendu et droit d'accès au dossier

1. Avant d'adopter une décision au titre de l'article 8, de l'article 9, paragraphe 1, de l'article 10, paragraphe 1, des articles 17, 18, 24, 25, 29 et 30 et de l'article 31, paragraphe 2, la Commission donne au contrôleur d'accès ou à l'entreprise ou à l'association d'entreprises concerné l'occasion de faire connaître son point de vue sur:

les constatations préliminaires de la Commission, y compris sur tout grief retenu par la Commission; et

a) les constatations préliminaires de la Commission, y compris sur tout grief retenu par la Commission; et

b) les mesures que la Commission peut avoir l'intention de prendre au vu des constatations préliminaires visées au point a) du présent paragraphe.a)

2. Les contrôleurs d'accès, les entreprises et les associations d'entreprises concernés peuvent présenter à la Commission leurs observations en ce qui concerne les constatations préliminaires de la Commission dans un délai fixé par la Commission dans ses constatations préliminaires et qui ne peut être inférieur à 14 jours.

3. La Commission ne fonde ses décisions que sur les constatations préliminaires, y compris sur tout grief retenu par la Commission, au sujet desquelles les contrôleurs d'accès, les entreprises et les associations d'entreprises concernés ont pu faire valoir leurs observations.

4. Les droits de la défense du contrôleur d'accès, de l'entreprise ou de l'association d'entreprises concerné sont pleinement assurés dans le déroulement de la procédure. Le contrôleur d'accès, l'entreprise ou l'association d'entreprises concerné a le droit d'avoir accès au dossier de la Commission conformément aux modalités de divulgation, sous réserve de l'intérêt légitime des entreprises à ce que leurs secrets d'affaires ne soient pas divulgués. En cas de désaccord entre les parties, la Commission peut adopter des décisions fixant ces modalités de divulgation. Le droit d'accès au dossier de la Commission ne s'étend pas aux informations confidentielles et aux documents internes de la Commission ou des autorités compétentes des États membres. En particulier, le droit d'accès ne s'étend pas à la correspondance entre la Commission et les autorités compétentes des États membres. Aucune disposition du présent paragraphe n'empêche la Commission de divulguer et d'utiliser des informations nécessaires pour apporter la preuve d'une infraction.

Article 35

Rapports annuels

1. La Commission présente au Parlement européen et au Conseil un rapport annuel sur la mise en œuvre du présent règlement et sur les progrès accomplis dans la réalisation de ses objectifs.

2. Le rapport visé au paragraphe 1 comprend:

a) un résumé des activités de la Commission, y compris toute mesure ou décision adoptée et les enquêtes de marché en cours en rapport avec le présent règlement;

b) les constatations résultant du suivi de la mise en œuvre par les contrôleurs d'accès des obligations au titre du présent règlement;

c) une évaluation de la description ayant fait l'objet d'un audit visée à l'article 15;

d) une vue d'ensemble de la coopération entre la Commission et les autorités nationales dans le cadre du présent règlement;

e) un aperçu des activités et des tâches effectuées par le groupe de haut niveau des régulateurs numériques, y compris la manière dont ses recommandations concernant l'application du présent règlement doivent être mises en œuvre.

3. La Commission publie le rapport sur son site internet.

Article 36

Secret professionnel

1. Les informations recueillies en vertu du présent règlement sont utilisées aux fins de celui-ci.

2. Les informations recueillies en vertu de l'article 14 sont utilisées aux fins du présent règlement, du règlement (CE) n° 139/2004 et des règles nationales en matière de concentration.

3. Les informations recueillies en vertu de l'article 15 sont utilisées aux fins du présent règlement et du règlement (UE) 2016/679.

4. Sans préjudice de l'échange et de l'utilisation des informations fournies aux fins d'utilisation selon les articles 38, 39, 41 et 43, la Commission, les autorités compétentes des États membres, leurs fonctionnaires, agents et les autres personnes travaillant sous la supervision de ces autorités, ainsi que toute personne physique ou morale, dont les auditeurs et experts nommés en vertu de l'article 26, paragraphe 2, sont tenus de ne pas divulguer les informations qu'ils ont recueillies ou échangées en application du présent règlement et qui, par leur nature, sont couvertes par le secret professionnel.

Article 37

Coopération avec les autorités nationales

1. La Commission et les États membres travaillent en étroite coopération et coordonnent leurs mesures d'exécution pour assurer une application cohérente, efficace et complémentaire des instruments juridiques disponibles appliqués aux contrôleurs d'accès au sens du présent règlement.

2. La Commission peut, le cas échéant, consulter les autorités nationales sur toute question relative à l'application du présent règlement.

Article 38

Coopération et coordination avec les autorités nationales compétentes chargées de faire appliquer les règles de concurrence

1. La Commission et les autorités nationales compétentes des États membres chargées de faire appliquer les règles visées à l'article 1er, paragraphe 6, coopèrent les unes avec les autres et s'échangent des informations sur leurs mesures d'exécution respectives par l'intermédiaire du Réseau européen de la concurrence (REC). Elles ont le pouvoir de se communiquer toute information relative à un élément de fait ou de droit, y compris s'il s'agit d'une information confidentielle. Si l'autorité compétente n'est pas membre du REC, la Commission établit les modalités nécessaires pour cette coopération et cet échange d'informations sur les dossiers concernant l'application du présent règlement et l'application des règles dans les cas visés à l'article 1er, paragraphe 6. La Commission peut établir ces modalités dans un acte d'exécution visé à l'article 46, paragraphe 1, point l).

2. Lorsqu'une autorité nationale compétente d'un État membre chargée de faire appliquer les règles visées à l'article 1er, paragraphe 6, a l'intention d'ouvrir une enquête sur des contrôleurs d'accès en application de dispositions législatives nationales visées à l'article 1er, paragraphe 6, elle informe la Commission par écrit de la première mesure d'enquête formelle, avant ou immédiatement après le début de cette mesure. Cette information peut également être mise à la disposition des autorités nationales compétentes chargées de faire appliquer les règles visées à l'article 1er, paragraphe 6, des autres États membres.

3. Lorsqu'une autorité nationale compétente d'un État membre chargée de faire appliquer les règles visées à l'article 1er, paragraphe 6, a l'intention d'imposer des obligations à des contrôleurs d'accès en application de dispositions législatives nationales visées à l'article 1er, paragraphe 6, elle communique le projet de mesure et ses motifs à la Commission, au plus tard 30 jours avant son adoption. Dans le cas de mesures provisoires, l'autorité nationale compétente d'un État membre chargée de faire appliquer les règles visées à l'article 1er, paragraphe 6, communique à la Commission les projets de mesures envisagées dès que possible et au plus tard immédiatement après l'adoption de ces mesures. Cette information peut également être mise à la disposition des autorités nationales compétentes chargées de faire appliquer les règles visées à l'article 1er, paragraphe 6, des autres États membres.

4. Les mécanismes d'information prévus aux paragraphes 2 et 3 ne s'appliquent pas aux décisions envisagées en vertu des règles nationales en matière de concentrations.

5. Les informations échangées en vertu des paragraphes 1 à 3 du présent article ne sont échangées et utilisées qu'aux fins de la coordination de l'application du présent règlement et des règles visées à l'article 1er, paragraphe 6.

6. La Commission peut demander aux autorités nationales compétentes des États membres chargées de faire appliquer les règles visées à l'article 1er, paragraphe 6, de soutenir toute enquête de marché qu'elle mène en application du présent règlement.

7. Lorsque, en vertu du droit national, une autorité nationale compétente d'un État membre chargée de faire appliquer les règles visées à l'article 1er, paragraphe 6, dispose de la compétence et des pouvoirs d'enquête voulus, elle peut, de sa propre initiative, mener une enquête sur un cas de non-respect éventuel des articles 5, 6 et 7 du présent règlement sur son territoire. Avant de prendre une première mesure d'enquête formelle, cette autorité en informe la Commission par écrit.

L'ouverture d'une procédure par la Commission en vertu de l'article 20 enlève aux autorités nationales compétentes des États membres chargées de contrôler le respect des règles visées à l'article 1er, paragraphe 6, la possibilité de mener une telle enquête ou de la clôturer lorsqu'elle est déjà en cours. Ces autorités communiquent à la Commission les résultats de l'enquête en question afin d'appuyer la Commission dans son rôle de seule instance habilitée à faire appliquer le présent règlement.

Article 39

Coopération avec les juridictions nationales

1. Dans le cadre des procédures engagées pour l'application du présent règlement, les juridictions nationales peuvent demander à la Commission de leur transmettre des informations en sa possession ou son avis sur des questions relatives à l'application du présent règlement.

2. Les États membres transmettent à la Commission une copie de toute décision écrite des juridictions nationales statuant sur l'application du présent règlement. Cette copie est transmise sans tarder lorsque le jugement complet est notifié par écrit aux parties.

3. Lorsqu'une application cohérente du présent règlement l'exige, la Commission, agissant de sa propre initiative, peut présenter des observations écrites aux juridictions nationales. Avec l'autorisation de la juridiction concernée, elle peut aussi présenter des observations orales.

4. Aux seules fins de l'élaboration de ses observations, la Commission peut demander à la juridiction nationale concernée de lui transmettre ou de lui faire transmettre tout document nécessaire à l'appréciation de l'affaire.

5. Les juridictions nationales ne prennent aucune décision qui va à l'encontre d'une décision adoptée par la Commission en vertu du présent règlement. Elles évitent également de prendre des décisions qui iraient à l'encontre d'une décision envisagée par la Commission dans une procédure qu'elle a intentée en vertu du présent règlement. À cette fin, la juridiction nationale peut évaluer s'il est nécessaire de suspendre sa procédure. Cette disposition est sans préjudice de la possibilité qu'ont les juridictions nationales d'introduire une demande de décision préjudicielle conformément à l'article 267 du traité sur le fonctionnement de l'Union européenne.

Article 40

Le groupe de haut niveau

1. La Commission met en place un groupe de haut niveau pour le règlement sur les marchés numériques (ci-après dénommé «groupe de haut niveau»).

2. Le groupe de haut niveau se compose des organes et réseaux européens suivants:

a) l'organe des régulateurs européens des communications électroniques,

b) le Contrôleur européen de la protection des données et le comité européen de la protection des données,

c) le réseau européen de la concurrence,

d) le réseau de coopération en matière de protection des consommateurs, et

e) le groupe des régulateurs européens pour les services de médias audiovisuels.

3. Les organes et réseaux européens visés au paragraphe 2 ont chacun un nombre égal de représentants au sein du groupe de haut niveau. Le nombre maximal de membres du groupe de haut niveau ne dépasse pas trente personnes.

4. La Commission fournit des services de secrétariat au groupe de haut niveau afin de faciliter ses travaux. Le groupe de haut niveau est présidé par la Commission, qui participe à ses réunions. Le groupe de haut niveau se réunit à la demande de la Commission au moins une fois par année civile. La Commission convoque également une réunion du groupe à la demande de la majorité des membres qui le composent afin de traiter une question spécifique.

5. Le groupe de haut niveau peut fournir à la Commission des conseils et une expertise dans les domaines relevant de la compétence de ses membres, notamment:

a) des conseils et des recommandations relevant de leur expertise et présentant un intérêt pour toute question générale quant à la mise en œuvre ou à l'application du présent règlement; ou

b) des conseils et une expertise en faveur d'une approche réglementaire cohérente entre les différents instruments réglementaires.

6. Le groupe de haut niveau peut, en particulier, recenser et évaluer les interactions actuelles et potentielles entre le présent règlement et les règles sectorielles appliquées par les autorités nationales composant les organismes et réseaux européens visés au paragraphe 2 et soumettre à la Commission un rapport annuel présentant cette évaluation et recensant les éventuels problèmes transréglementaires. Ce rapport peut être accompagné de recommandations visant à converger vers des approches transdisciplinaires cohérentes et des synergies entre la mise en œuvre du présent règlement et celle d'autres réglementations sectorielles. Ce rapport est communiqué au Parlement européen et au Conseil.

7. Dans le cadre d'enquêtes de marché sur de nouveaux services et de nouvelles pratiques, le groupe de haut niveau peut apporter son expertise à la Commission sur la nécessité de modifier, d'ajouter ou de supprimer des règles figurant dans le présent règlement afin de faire en sorte que les marchés numériques dans l'ensemble de l'Union soient contestables et équitables.

Article 41

Demande d'enquête de marché

1. Trois États membres ou plus peuvent solliciter auprès de la Commission l'ouverture d'une enquête de marché conformément à l'article 17 parce qu'il existe, selon eux, des motifs raisonnables de soupçonner qu'une entreprise devrait être désignée comme contrôleur d'accès.

2. Un ou plusieurs États membres peuvent demander à la Commission d'ouvrir une enquête de marché conformément à l'article 18 parce qu'il existe, selon eux, des motifs raisonnables de soupçonner qu'un contrôleur d'accès a systématiquement contrevenu à une ou plusieurs des obligations prévues aux articles 5, 6 et 7, et qu'il a maintenu, renforcé ou étendu sa position de contrôleur d'accès au regard des caractéristiques énoncées à l'article 3, paragraphe 1.

3. Trois États membres ou plus peuvent solliciter auprès de la Commission l'ouverture d'une enquête de marché conformément à l'article 19 parce qu'il existe, selon eux, des motifs raisonnables de soupçonner:

a) qu'il faudrait ajouter davantage de services relevant du secteur numérique à la liste des services de plateforme essentiels établie à l'article 2, point 2); ou

b) que le présent règlement ne permet pas de remédier de manière effective à une ou plusieurs pratiques et que ces pratiques sont susceptibles de limiter la contestabilité des service de plateforme essentiels ou d'être inéquitables.

4. Les États membres apportent des éléments de preuve à l'appui de leurs demandes introduites en vertu des paragraphes 1, 2 et 3. Pour les demandes introduites en vertu du paragraphe 3, ces éléments de preuve peuvent inclure des informations sur les offres nouvelles de produits, de services, de logiciels ou de fonctionnalités qui suscitent des préoccupations du point de vue de la contestabilité ou de l'équité, qu'elles soient mises en œuvre dans le cadre de services de plateforme essentiels existants ou d'une autre façon.

5. Dans les quatre mois suivant la réception d'une demande introduite en vertu du présent article, la Commission examine s'il existe des motifs raisonnables pour ouvrir une enquête de marché en vertu du paragraphe 1, 2 ou 3. La Commission publie les résultats de cette évaluation.

Article 42

Actions représentatives

La directive (UE) 2020/1828 est applicable aux actions représentatives intentées en raison des infractions commises par des contrôleurs d'accès aux dispositions du présent règlement qui portent atteinte ou risquent de porter atteinte aux intérêts collectifs des consommateurs.

Article 43

Signalement de violations et protection des auteurs de signalement

Le signalement de toutes les violations du présent règlement et la protection des personnes signalant ces violations sont régis par la directive (UE) 2019/1937.

CHAPITRE VI
DISPOSITIONS FINALES

Article 44

Publication des décisions

1. La Commission publie les décisions qu'elle prend au titre des articles 3 et 4, de l'article 8, paragraphe 2, des articles 9, 10, 16 à 20 et 24, de l'article 25, paragraphe 1, et des articles 29, 30 et 31. Cette publication mentionne le nom des parties intéressées et l'essentiel de la décision, y compris les sanctions imposées.

2. La publication tient compte de l'intérêt légitime des contrôleurs d'accès ou des tiers à ce que leurs informations confidentielles ne soient pas divulguées.

Article 45

Contrôle de la Cour de justice

Conformément à l'article 261 du traité sur le fonctionnement de l'Union européenne, la Cour de justice statue avec compétence de pleine juridiction sur les recours dirigés contre les décisions par lesquelles la Commission inflige des amendes ou des astreintes. Elle peut supprimer, réduire ou majorer l'amende ou l'astreinte infligée.

Article 46

Dispositions d'exécution

1. La Commission peut adopter des actes d'exécution établissant les modalités détaillées pour l'application de ce qui suit:

a) la forme, la teneur et les autres modalités des notifications et mémoires présentés en application de l'article 3;

b) la forme, la teneur et les autres modalités des mesures techniques que les contrôleurs d'accès mettent en œuvre pour garantir le respect de l'article 5, 6 ou 7;

c) les modalités opérationnelles et techniques en vue de la mise en œuvre de l'interopérabilité des services de communications interpersonnelles non fondés sur la numérotation conformément à l'article 7;

d) la forme, la teneur et les autres modalités de la demande motivée présentée en application de l'article 8, paragraphe 3;

e) la forme, la teneur et les autres modalités des demandes motivées présentées en application des articles 9 et 10;

f) la forme, la teneur et les autres modalités des rapports réglementaires communiqués en application de l'article 11;

g) la méthodologie et la procédure pour la description, devant faire l'objet d'un audit, des techniques utilisées pour le profilage des consommateurs prévue à l'article 15, paragraphe 1; lorsqu'elle élabore un projet d'acte d'exécution à cette fin, la Commission consulte le Contrôleur européen de la protection des données et peut consulter le comité européen de la protection des données, la société civile et d'autres experts compétents;

h) la forme, la teneur et les autres modalités des notifications et mémoires présentés en application des articles 14 et 15;

i) les modalités des procédures relatives aux enquêtes de marché prévues aux articles 17, 18 et 19 et des procédures définies aux articles 24, 25 et 29;

j) les modalités d'exercice du droit d'être entendu prévu à l'article 34;

k) les modalités pour les conditions de la divulgation prévue à l'article 34;

l) les modalités de la coopération et de la coordination entre la Commission et les autorités nationales prévues aux articles 37 et 38; et

m) les modalités de calcul et de prolongation des délais.

2. Les actes d'exécution visés au paragraphe 1, points a) à k) et m), du présent article sont adoptés en conformité avec la procédure consultative visée à l'article 50, paragraphe 2.

L'acte d'exécution visé au paragraphe 1, point l), du présent article est adopté en conformité avec la procédure d'examen visée à l'article 50, paragraphe 3.

3. Avant l'adoption de tout acte d'exécution en vertu du paragraphe 1, la Commission en publie le projet et invite toutes les parties intéressées à lui soumettre leurs observations dans un délai qui ne peut être inférieur à un mois.

Article 47

Lignes directrices

La Commission peut adopter des lignes directrices sur tout aspect du présent règlement afin de faciliter sa mise en œuvre et son application effectives.

Article 48

Normalisation

Si elle le juge opportun et nécessaire, la Commission peut charger les organisations européennes de normalisation d'élaborer des normes appropriées pour faciliter la mise en œuvre des obligations fixées dans le présent règlement.

Article 49

Exercice de la délégation

1. Le pouvoir d'adopter des actes délégués conféré à la Commission est soumis aux conditions fixées au présent article.

2. Le pouvoir d'adopter des actes délégués visé à l'article 3, paragraphes 6 et 7, et à l'article 12, paragraphes 1, 3 et 4, est conféré à la Commission pour une période de cinq ans à compter du 1er novembre 2022. La Commission élabore un rapport relatif à la délégation de pouvoir au plus tard neuf mois avant la fin de la période de cinq ans. La délégation de pouvoir est tacitement prorogée pour des périodes d'une durée identique, sauf si le Parlement européen ou le Conseil s'oppose à cette prorogation trois mois au plus tard avant la fin de chaque période.

3. La délégation de pouvoir visée à l'article 3, paragraphes 6 et 7, et à l'article 12, paragraphes 1, 3 et 4, peut être révoquée à tout moment par le Parlement européen ou le Conseil. La décision de révocation met fin à la délégation de pouvoir qui y est précisée. La révocation prend effet le jour suivant celui de la publication de ladite décision au *Journal officiel de l'Union européenne* ou à une date ultérieure qui est précisée dans ladite décision. Elle ne porte pas atteinte à la validité des actes délégués déjà en vigueur.

4. Avant l'adoption d'un acte délégué, la Commission consulte les experts désignés par chaque État membre, conformément aux principes définis dans l'accord interinstitutionnel du 13 avril 2016«Mieux légiférer».

5. Aussitôt qu'elle adopte un acte délégué, la Commission le notifie au Parlement européen et au Conseil simultanément.

6. Un acte délégué adopté en vertu de l'article 3, paragraphes 6 et 7, et de l'article 12, paragraphes 1, 3 et 4, n'entre en vigueur que si le Parlement européen ou le Conseil n'a pas exprimé d'objections dans un délai de deux mois à compter de la notification de cet acte au Parlement européen et au Conseil ou si, avant l'expiration de ce délai, le Parlement européen et le Conseil ont tous deux informé la Commission de leur intention de ne pas exprimer d'objections. Ce délai est prolongé de deux mois à l'initiative du Parlement européen ou du Conseil.

Article 50

Comité

1. La Commission est assistée par un comité (ci-après dénommé «comité consultatif en matière de marchés numériques»). Ledit comité est un comité au sens du règlement (UE) n° 182/2011.

2. Lorsqu'il est fait référence au présent paragraphe, l'article 4 du règlement (UE) n° 182/2011 s'applique.

Lorsque l'avis du comité doit être obtenu par procédure écrite, ladite procédure est close sans résultat lorsque, dans le délai pour émettre un avis, le président du comité le décide ou une majorité simple des membres du comité le demandent.

3. Lorsqu'il est fait référence au présent paragraphe, l'article 5 du règlement (UE) n° 182/2011 s'applique.

4. La Commission fait part au destinataire d'une décision individuelle de l'avis du comité, accompagné de cette décision. Elle rend publics l'avis et la décision individuelle, en tenant compte de l'intérêt légitime à la protection du secret professionnel.

Article 51

Modification de la directive (UE) 2019/1937

À la partie I, point J, de l'annexe de la directive (UE) 2019/1937, le point suivant est ajouté:

«iv) 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 (règlement sur les marchés numériques) (JO L 265 du 21.9.2022, p. 1).».

Article 52

Modification de la directive (UE) 2020/1828

À l'annexe I de la directive (UE) 2020/1828, le point suivant est ajouté:

«67) 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 (règlement sur les marchés numériques) (JO L 265 du 21.9.2022, p. 1).».

Article 53

Réexamen

1. Au plus tard le 3 mai 2026, et tous les trois ans par la suite, la Commission évalue le présent règlement et fait rapport au Parlement européen, au Conseil et au Comité économique et social.

2. Les évaluations déterminent si les objectifs du présent règlement consistant à garantir que les marchés soient contestables et équitables ont été atteints, et elles mesurent l'incidence du présent règlement pour les entreprises utilisatrices, notamment les PME, et les utilisateurs finaux. De plus, la Commission évalue si le champ de l'article 7 peut être élargi aux services de réseaux sociaux en ligne.

3. Les évaluations déterminent s'il est nécessaire de modifier les règles, notamment en ce qui concerne la liste des services de plateforme essentiels établie à l'article 2, point 2), les obligations prévues aux articles 5, 6 et 7 et le contrôle de leur respect, afin de garantir la contestabilité et l'équité des marchés numériques dans l'Union. À la suite des évaluations, la Commission prend les mesures appropriées, qui peuvent comprendre des propositions législatives.

4. Les autorités compétentes des États membres communiquent toutes les informations pertinentes dont elles disposent que la Commission pourrait solliciter aux fins de l'établissement du rapport visé au paragraphe 1.

Article 54

Entrée en vigueur et application

Le présent règlement entre en vigueur le vingtième jour suivant celui de sa publication au *Journal officiel de l'Union européenne*.

Il est applicable à partir du 2 mai 2023.

Cependant, l'article 3, paragraphes 6 et 7, ainsi que les articles 40, 46, 47, 48, 49 et 50 sont applicables à partir du 1er novembre 2022, et les articles 42 et 43 sont applicables à partir du 25 juin 2023.

Toutefois, si la date du 25 juin 2023 précède la date d'application visée au deuxième alinéa du présent article, l'application des articles 42 et 43 est repoussée à la date d'application visée au deuxième alinéa du présent article.
Le présent règlement est obligatoire dans tous ses éléments et directement applicable dans tout État membre.

Fait à Strasbourg, le 14 septembre 2022

Par le Parlement européen

La présidente

R. METSOLA

Par le Conseil

Le président

M. BEK

(1) JO C 286 du 16.7.2021, p. 64.

(2) JO C 440 du 29.10.2021, p. 67.

(3) Position du Parlement européen du 5 juillet 2022 (non encore parue au Journal officiel) et décision du Conseil du 18 juillet 2022.

(4) 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) (JO L 119 du 4.5.2016, p. 1).

(5) Règlement (UE) 2019/1150 du Parlement européen et du Conseil du 20 juin 2019 promouvant l'équité et la transparence pour les entreprises utilisatrices de services d'intermédiation en ligne (JO L 186 du 11.7.2019, p. 57).

(6) Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques) (JO L 201 du 31.7.2002, p. 37).

(7) Directive 2005/29/CE du Parlement européen et du Conseil du 11 mai 2005 relative aux pratiques commerciales déloyales des entreprises vis-à-vis des consommateurs dans le marché intérieur et modifiant la directive 84/450/CEE du Conseil et les directives 97/7/CE, 98/27/CE et 2002/65/CE du Parlement européen et du Conseil et le règlement (CE) n° 2006/2004 du Parlement européen et du Conseil («directive sur les pratiques commerciales déloyales») (JO L 149 du 11.6.2005, p. 22).

(8) Directive 2010/13/UE du Parlement européen et du Conseil du 10 mars 2010 visant à la coordination de certaines dispositions législatives, réglementaires et administratives des États membres relatives à la fourniture de services de médias audiovisuels (directive «Services de médias audiovisuels») (JO L 95 du 15.4.2010, p. 1).

(9) Directive (UE) 2015/2366 du Parlement européen et du Conseil du 25 novembre 2015 concernant les services de paiement dans le marché intérieur, modifiant les directives 2002/65/CE, 2009/110/CE et 2013/36/UE et le règlement (UE) n° 1093/2010, et abrogeant la directive 2007/64/CE (JO L 337 du 23.12.2015, p. 35).

(10) Directive (UE) 2019/790 du Parlement européen et du Conseil du 17 avril 2019 sur le droit d'auteur et les droits voisins dans le marché unique numérique et modifiant les directives 96/9/CE et 2001/29/CE (JO L 130 du 17.5.2019, p. 92).

(11) Directive (UE) 2019/882 du Parlement européen et du Conseil du 17 avril 2019 relative aux exigences en matière d'accessibilité applicables aux produits et services (JO L 151 du 7.6.2019, p. 70).

(12) Directive 93/13/CEE du Conseil du 5 avril 1993 concernant les clauses abusives dans les contrats conclus avec les consommateurs (JO L 95 du 21.4.1993, p. 29).

(13) Directive (UE) 2015/1535 du Parlement européen et du Conseil du 9 septembre 2015 prévoyant une procédure d'information dans le domaine des réglementations techniques et des règles relatives aux services de la société de l'information (JO L 241 du 17.9.2015, p. 1).

(14) Directive (UE) 2018/1972 du Parlement européen et du Conseil du 11 décembre 2018 établissant le code des communications électroniques européen (JO L 321 du 17.12.2018, p. 36).

(15) Directive (UE) 2016/2102 du Parlement européen et du Conseil du 26 octobre 2016 relative à l'accessibilité des sites internet et des applications mobiles des organismes du secteur public (JO L 327 du 2.12.2016, p. 1).

(16) Règlement (UE) n° 182/2011 du Parlement européen et du Conseil du 16 février 2011 établissant les règles et principes généraux relatifs aux modalités de contrôle par les États membres de l'exercice des compétences d'exécution par la Commission (JO L 55 du 28.2.2011, p. 13).

(17) Règlement (UE) 2018/1725 du Parlement européen et du Conseil du 23 octobre 2018 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union et à la libre circulation de ces données, et abrogeant le règlement (CE) n° 45/2001 et la décision n° 1247/2002/CE (JO L 295 du 21.11.2018, p. 39).

(18) Règlement (CE) n° 1/2003 du Conseil du 16 décembre 2002 relatif à la mise en œuvre des règles de concurrence prévues aux articles 81 et 82 du traité (JO L 1 du 4.1.2003, p. 1).

(19) JO L 123 du 12.5.2016, p. 1.

(20) Directive (UE) 2019/1937 du Parlement européen et du Conseil du 23 octobre 2019 sur la protection des personnes qui signalent des violations du droit de l'Union (JO L 305 du 26.11.2019, p. 17).

(21) Directive (UE) 2020/1828 du Parlement européen et du Conseil du 25 novembre 2020 relative aux actions représentatives visant à protéger les intérêts collectifs des consommateurs et abrogeant la directive 2009/22/CE (JO L 409 du 4.12.2020, p. 1).

(22) JO C 147 du 26.4.2021, p. 4.

(23) Règlement (CE) n° 139/2004 du Conseil du 20 janvier 2004 relatif au contrôle des concentrations entre entreprises («le règlement CE sur les concentrations») (JO L 24 du 29.1.2004, p. 1).

(24) Directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union (JO L 194 du 19.7.2016, p. 1).

ANNEXE

A. Généralités

1. La présente annexe vise à préciser la méthode d'identification et de calcul des «utilisateurs finaux actifs» et des «entreprises utilisatrices actives» pour chaque service de plateforme essentiel énumérés à l'article 2, point 2). Elle fournit une référence permettant à une entreprise d'évaluer si ses services de plateforme essentiels respectent les seuils quantitatifs fixés à l'article 3, paragraphe 2, point b), et sont donc présumés satisfaire à l'exigence énoncée à l'article 3, paragraphe 1, point b). Cette référence sera donc également pertinente pour toute appréciation plus large au titre de l'article 3, paragraphe 8. Il incombe à l'entreprise de parvenir à la meilleure estimation possible, conformément aux principes communs et à la méthode spécifique énoncés dans la présente annexe. Aucune disposition de la présente annexe n'empêche la Commission, dans les délais fixés par les dispositions pertinentes du présent règlement, d'exiger de l'entreprise fournissant des services de plateforme essentiels qu'elle fournisse toutes les informations nécessaires pour identifier les «utilisateurs finaux actifs» et les «entreprises utilisatrices actives» et en calculer le nombre. Aucune disposition de la présente annexe ne devrait constituer une base juridique pour le traçage des utilisateurs. La méthode figurant dans la présente annexe est également sans préjudice de l'une quelconque des obligations fixées par le présent règlement, notamment celles énoncées à l'article 3, paragraphes 3 et 8, et à l'article 13, paragraphe 3. En particulier, le respect de l'article 13, paragraphe 3, signifie également qu'il convient d'identifier les «utilisateurs finaux actifs» et les «entreprises utilisatrices actives» et d'en calculer le nombre sur la base d'une mesure précise ou de la meilleure estimation possible, conformément aux capacités réelles d'identification et de calcul dont dispose au moment voulu l'entreprise fournissant des services de plateforme essentiels. Ces mesures ou la meilleure estimation possible doivent être cohérentes avec les informations communiquées en vertu de l'article 15 et les inclure.

2. À l'article 2, les points 20) et 21) énoncent les définitions d'«utilisateur final» et d'«entreprise utilisatrice», qui sont communes à tous les services de plateforme essentiels.

3. Afin d'identifier les «utilisateurs finaux actifs» et les «entreprises utilisatrices actives» et d'en calculer le nombre, la présente annexe fait référence à la notion d'«utilisateurs uniques». La notion d'«utilisateurs uniques» recouvre les «utilisateurs finaux actifs» et les «entreprises utilisatrices actives» comptabilisés une seule fois, pour le service de plateforme essentiel concerné, pour une période donnée (c'est-à-dire par mois dans le cas des «utilisateurs finaux actifs» et par année dans le cas des «entreprises utilisatrices actives»), indépendamment du nombre de leurs interactions avec le service de plateforme essentiel concerné au cours de cette période. Cela est sans préjudice du fait que la même personne physique ou morale peut simultanément constituer un «utilisateur final actif» ou une «entreprise utilisatrice active» pour différents services de plateforme essentiels.

B. «Utilisateurs finaux actifs»

1. Le nombre d'«utilisateurs uniques» au regard des «utilisateurs finaux actifs» est établi en fonction de la mesure la plus précise déclarée par l'entreprise fournissant l'un des services de plateforme essentiels, en particulier:

a) On considère que la collecte de données sur l'utilisation des services de plateforme essentiels à partir d'environnements fonctionnant par inscription ou connexion présenterait, à première vue, le risque le plus faible de duplication, par exemple concernant le comportement des utilisateurs sur l'ensemble des appareils ou des plateformes. Par conséquent, l'entreprise soumet des données anonymisées agrégées sur le nombre d'utilisateurs finaux uniques par service de plateforme essentiel concerné sur la base des environnements fonctionnant par inscription ou connexion, si de telles données existent.

b) Dans le cas des services de plateforme essentiels auxquels des utilisateurs finaux ont également accès en dehors des environnements fonctionnant par inscription ou connexion, l'entreprise soumet en outre des données anonymisées agrégées sur le nombre d'utilisateurs finaux uniques du service de plateforme essentiel concerné, sur la base d'une autre mesure prenant en compte également les utilisateurs finaux en dehors des environnements fonctionnant par inscription ou connexion, tels que les adresses de protocole internet, les témoins de connexion (cookies) ou d'autres identifiants tels que les étiquettes d'identification par radiofréquence, pour autant que ces adresses ou témoins de connexion soient objectivement nécessaires à la fourniture de services de plateforme essentiels.

2. Le nombre d'«utilisateurs finaux actifs par mois» est fondé sur le nombre moyen d'utilisateurs finaux actifs chaque mois durant la majeure partie de l'exercice. La notion de «majeure partie de l'exercice» vise à permettre à une entreprise fournissant des services de plateforme essentiels d'écarter des valeurs exceptionnelles au cours d'une année donnée. On entend par valeurs exceptionnelles celles qui sortent nettement de ce qui ressort de l'ordinaire et du prévisible. Une situation où, de manière inattendue, au cours d'un seul mois de l'exercice, la participation des utilisateurs atteindrait un niveau record ou connaîtrait une forte baisse est un exemple de ce qui pourrait constituer de telles valeurs exceptionnelles. Les valeurs en rapport avec des événements intervenant chaque année, tels que les promotions annuelles des ventes, ne constituent pas des valeurs exceptionnelles.

C. «Entreprises utilisatrices actives»

Le nombre d'«utilisateurs uniques» au regard des «entreprises utilisatrices actives» doit être déterminé, s'il y a lieu, au niveau du compte, chaque compte d'entreprise distinct, associé à l'utilisation d'un service de plateforme essentiel fourni par l'entreprise, constituant une entreprise utilisatrice unique de ce service de plateforme essentiel. Si la notion de «compte d'entreprise» ne s'applique pas à un service de plateforme essentiel donné, l'entreprise concernée fournissant des services de plateforme essentiels détermine le nombre d'entreprises utilisatrices uniques en se référant à l'entreprise concernée.

D. Communication d'informations

1. L'entreprise qui communique à la Commission, conformément à l'article 3, paragraphe 3, des informations concernant le nombre d'utilisateurs finaux actifs et d'entreprises utilisatrices actives par service de plateforme essentiel est chargée de veiller à l'exhaustivité et à l'exactitude de ces informations. À cet égard:

a) l'entreprise est tenue de transmettre les données pour un service de plateforme essentiel donné en évitant de sous-évaluer ou de surévaluer le nombre d'utilisateurs finaux actifs et d'entreprises utilisatrices actives (par exemple, lorsque les utilisateurs accèdent aux services de plateforme essentiels à partir de différentes plateformes ou de différents appareils);

b) l'entreprise est tenue de fournir des explications précises et succinctes sur la méthode utilisée pour obtenir les informations fournies et elle est responsable de tout risque de sous-évaluation ou de surévaluation du nombre d'utilisateurs finaux actifs et d'entreprises utilisatrices actives pour un service de plateforme essentiel donné et des solutions adoptées pour remédier à ce risque;

c) l'entreprise fournit des données basées sur une autre méthode de mesure lorsque la Commission a des doutes quant à l'exactitude des données fournies par l'entreprise fournissant les services de plateforme essentiels.

2. Aux fins du calcul du nombre d'«utilisateurs finaux actifs» et d'«entreprises utilisatrices actives»:

a) l'entreprise fournissant un ou des services de plateforme essentiels ne répertorie pas les services de plateforme essentiels appartenant à une même catégorie de services de plateforme essentiels définis à l'article 2, point 2), comme étant distincts en se basant principalement sur le fait qu'ils sont fournis en utilisant des noms de domaine différents, qu'il s'agisse de domaines de premier niveau nationaux (ccTLD) ou de domaines de premier niveau génériques (gTLD), ou sur tout attribut géographique;

b) l'entreprise fournissant un ou des services de plateforme essentiels considère comme distincts les services de plateforme essentiels qui sont utilisés à des fins différentes soit par leurs utilisateurs finaux, soit par leurs entreprises utilisatrices, soit encore par les deux, même si leurs utilisateurs finaux ou leurs entreprises utilisatrices peuvent être identiques et même s'ils appartiennent à la même catégorie de services de plateforme essentiels définis à l'article 2, point 2);

c) l'entreprise fournissant un ou des services de plateforme essentiels considère comme étant des services de plateforme essentiels distincts les services que l'entreprise concernée propose de manière intégrée, mais qui:

i) n'appartiennent pas à la même catégorie de services de plateforme essentiels définis à l'article 2, point 2), ou

ii) sont utilisés à des fins différentes soit par leurs utilisateurs finaux, soit par leurs entreprises utilisatrices, soit encore par les deux, même si leurs utilisateurs finaux ou leurs entreprises utilisatrices peuvent être identiques et même s'ils appartiennent à

la même catégorie de services de plateforme essentiels en vertu de l'article 2, point 2).

E. «Définitions spécifiques»

Le tableau ci-dessous contient des définitions spécifiques des notions d'«utilisateurs finaux actifs» et d'«entreprises utilisatrices actives» pour chaque service de plateforme essentiel.

Services de plateforme essentiels	Utilisateurs finaux actifs	Entreprises utilisatrices actives
Services d'intermédiation en ligne	Nombre d'utilisateurs finaux uniques qui, au moins une fois pendant le mois, ont interagi avec le service d'intermédiation en ligne, par exemple en se connectant, en effectuant une recherche, en cliquant ou en utilisant le défilement de manière active, ou qui, au moins une fois pendant le mois, ont conclu une transaction via le service d'intermédiation en ligne.	Nombre d'entreprises utilisatrices uniques dont au moins un article a figuré sur une liste dans le service d'intermédiation en ligne pendant toute l'année ou qui, pendant l'année, ont conclu une transaction rendue possible par le service d'intermédiation en ligne.
Moteurs de recherche en ligne	Nombre d'utilisateurs finaux uniques qui, au moins une fois pendant le mois, ont interagi avec le moteur de recherche en ligne, par exemple en effectuant une recherche.	Nombre d'entreprises utilisatrices uniques disposant de sites internet commerciaux (c'est-à-dire de sites internet utilisés à des fins commerciales ou professionnelles) qui sont indexés par le moteur de recherche en ligne ou font partie de l'index du moteur de recherche en ligne pendant l'année.
Services de réseaux sociaux en ligne	Nombre d'utilisateurs finaux uniques qui ont interagi avec le service de réseau social en ligne au moins une fois pendant le mois, par exemple en se connectant, en ouvrant une page, en utilisant le défilement, en cliquant, en utilisant la fonction «Like/J'aime», en lançant une recherche, en publiant ou en commentant, de manière active.	Nombre d'entreprises utilisatrices uniques qui sont inscrites sur la liste d'entreprises ou disposent d'un compte d'entreprise dans le service de réseau social en ligne et qui ont interagi avec le service, de quelque manière que ce soit, au moins une fois pendant l'année, par exemple en se connectant, en ouvrant une page, en utilisant le défilement, en cliquant, en utilisant la fonction «Like/J'aime», en effectuant une recherche, en publiant, en commentant ou en utilisant ses outils pour les entreprises, de manière active.

Services de plateformes de partage de vidéos	Nombre d'utilisateurs finaux uniques qui ont interagi avec le service de plateforme de partage de vidéos au moins une fois pendant le mois, par exemple en diffusant un segment de contenu audiovisuel, en effectuant une recherche ou en téléchargeant un contenu audiovisuel vers la plateforme, y compris des vidéos créées par les utilisateurs.	Nombre d'entreprises utilisatrices uniques qui, pendant l'année, ont fourni au moins un contenu audiovisuel téléchargé vers le service de la plateforme de partage de vidéos ou diffusé sur celle-ci.
Services de communications interpersonnelles non fondés sur la numérotation	Nombre d'utilisateurs finaux uniques qui, au moins une fois pendant le mois, ont lancé d'une manière ou d'une autre une communication ou y ont participé par l'intermédiaire du service de communications interpersonnelles non fondé sur la numérotation.	Nombre d'entreprises utilisatrices uniques qui, au moins une fois pendant l'année, ont utilisé un compte d'entreprise ou qui ont, de n'importe quelle autre manière, lancé une communication ou, de quelque façon que ce soit, y ont participé par l'intermédiaire du service de communication interpersonnelle non fondé sur la numérotation pour communiquer directement avec un utilisateur final.
Systèmes d'exploitation	Nombre d'utilisateurs finaux uniques qui ont utilisé un dispositif équipé du système d'exploitation ayant été activé, mis à jour ou utilisé au moins une fois pendant le mois.	Nombre de développeurs uniques qui, pendant l'année, ont publié, mis à jour ou proposé au moins une application ou un programme logiciel utilisant le langage de programmation ou tout outil de développement logiciel du système d'exploitation ou fonctionnant de quelque manière que ce soit sur le système d'exploitation.
Assistant virtuel	Nombre d'utilisateurs finaux uniques qui, au moins une fois pendant le mois, ont interagi avec l'assistant virtuel de quelque manière que ce soit, par exemple en l'activant, en posant une question, en accédant à un service par une commande ou en contrôlant un dispositif de maison intelligente.	Nombre de développeurs uniques qui, au cours de l'année, ont proposé au moins une application logicielle d'assistant virtuel ou une fonctionnalité permettant de rendre une application logicielle existante accessible par l'intermédiaire de l'assistant virtuel.
Navigateurs internet	Nombre d'utilisateurs finaux uniques qui, au moins une fois pendant le mois, ont interagi avec le navigateur internet, par exemple en insérant une requête ou une adresse de site internet dans la ligne URL du navigateur internet.	Nombre d'entreprises utilisatrices uniques dont les sites internet d'entreprise (c'est-à-dire les sites internet utilisés à des fins commerciales ou professionnelles) ont, au moins une fois pendant le mois, été consultés par l'intermédiaire du navigateur internet ou qui ont proposé un plug-in, une extension ou des outils

		complémentaires utilisés sur le navigateur internet au cours de l'année.
Services d'informatique en nuage	Nombre d'utilisateurs finaux uniques qui, au moins une fois pendant le mois, ont interagi avec des services d'informatique en nuage fournis par le fournisseur concerné de services d'informatique en nuage, en échange de tout type de rémunération, que celle-ci ait eu lieu ou non le même mois.	Nombre d'entreprises utilisatrices uniques qui, au cours de l'année, ont fourni tout service d'informatique en nuage hébergé dans l'infrastructure en nuage du fournisseur de services d'informatique en nuage concerné.
Services de publicité en ligne	Pour les ventes propriétaires d'espaces publicitaires: Nombre d'utilisateurs finaux uniques qui, au moins une fois pendant le mois, ont été exposés à une publicité. Pour les services d'intermédiation publicitaire (y compris les réseaux publicitaires, les échanges publicitaires et tout autre service d'intermédiation publicitaire): Nombre d'utilisateurs finaux uniques qui, au moins une fois pendant le mois, ont été exposés à une publicité ayant déclenché le service d'intermédiation publicitaire.	Pour les ventes propriétaires d'espaces publicitaires: Nombre d'annonceurs uniques dont au moins une publicité a été exposée pendant l'année. Pour les services d'intermédiation publicitaire (y compris les réseaux publicitaires, les échanges publicitaires et tout autre service d'intermédiation publicitaire): Nombre d'entreprises utilisatrices uniques (y compris les annonceurs, les éditeurs ou d'autres intermédiaires) qui, au cours de l'année, ont interagi via le service d'intermédiation publicitaire ou ont eu recours à ses services.

Journal officiel de l’Union européenne

L 265/1

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 (règlement sur les marchés numériques)

(Texte présentant de l’intérêt pour l’EEE)

LE PARLEMENT EUROPÉEN ET LE CONSEIL DE L’UNION EUROPÉENNE,

vu le traité sur le fonctionnement de l’Union européenne, et notamment son article 114,

vu la proposition de la Commission européenne,

après transmission du projet d’acte législatif aux parlements nationaux,

vu l’avis du Comité économique et social européen (1),

vu l’avis du Comité des régions (2),

statuant conformément à la procédure législative ordinaire (3),

considérant ce qui suit:

(1)

Les services numériques en général et les plateformes en ligne en particulier jouent un rôle toujours plus important au sein de l’économie, notamment sur le marché intérieur, en permettant aux entreprises d’atteindre les utilisateurs dans l’ensemble de l’Union, en facilitant le commerce transfrontière et en ouvrant des débouchés commerciaux entièrement nouveaux à un grand nombre d’entreprises dans l’Union, au profit des consommateurs dans l’Union.

(2)

Parallèlement, parmi ces services numériques, les services de plateforme essentiels présentent un certain nombre de caractéristiques qui peuvent être exploitées par les entreprises qui les fournissent. Parmi les caractéristiques de ces services de plateforme essentiels figurent par exemple des économies d’échelle extrêmes, qui résultent souvent de coûts marginaux presque nuls pour ajouter des entreprises utilisatrices ou des utilisateurs finaux. Les services de plateforme essentiels se caractérisent en outre par des effets de réseau très importants, leur capacité de relier de nombreuses entreprises utilisatrices avec de nombreux utilisateurs finaux grâce à leur caractère multiface, un degré considérable de dépendance des entreprises utilisatrices et des utilisateurs finaux, des effets de verrouillage, l’absence de

multihébergement aux mêmes fins par les utilisateurs finaux, l'intégration verticale et les avantages liés aux données. Toutes ces caractéristiques, combinées à des pratiques déloyales de la part des entreprises fournissant ces services de plateforme essentiels, peuvent sensiblement compromettre la contestabilité des services de plateforme essentiels, ainsi que nuire à l'équité de la relation commerciale entre les entreprises fournissant ces services et leurs entreprises utilisatrices et utilisateurs finaux. En pratique, cela conduit à une diminution rapide et potentiellement considérable du choix des entreprises utilisatrices et utilisateurs finaux, et peut donc conférer au fournisseur de ces services la position de «contrôleurs d'accès». Dans le même temps, il convient de reconnaître que les services qui ne poursuivent pas d'objectif commercial, comme les projets collaboratifs, ne devraient pas être considérés comme des services de plateforme essentiels aux fins du présent règlement.

(3)

Un petit nombre de grandes entreprises fournissant des services de plateforme essentiels ont vu le jour et disposent d'un pouvoir économique considérable qui pourrait faire d'elles des contrôleurs d'accès au sens du présent règlement. En règle générale, elles sont en mesure de relier de nombreuses entreprises utilisatrices à de nombreux utilisateurs finaux à travers leurs services, ce qui, en retour, leur permet de tirer profit de leurs avantages, tels qu'un accès à de vastes quantités de données, d'un domaine d'activité à un autre. Certaines de ces entreprises exercent un contrôle sur des écosystèmes de plateformes entiers au sein de l'économie numérique et sont structurellement extrêmement difficiles à concurrencer ou à contester par des opérateurs du marché existants ou nouveaux, indépendamment du degré d'innovation et d'efficacité de ces opérateurs du marché. La contestabilité est réduite en particulier du fait de l'existence de barrières très hautes à l'entrée ou à la sortie, y compris des coûts d'investissement élevés qui, en cas de sortie, ne sont pas récupérables, ou le sont difficilement, et l'absence d'intrants clés de l'économie numérique, tels que les données, ou l'accès limité à ces derniers. Le mauvais fonctionnement des marchés sous-jacents, ou leur mauvais fonctionnement futur, est par conséquent plus probable.

(4)

Dans de nombreux cas, cette combinaison de caractéristiques des contrôleurs d'accès est susceptible de mener à de graves déséquilibres en matière de pouvoir de négociation, et donc à des pratiques et conditions déloyales à l'égard tant des entreprises utilisatrices que des utilisateurs finaux de services de plateforme essentiels fournis par ces contrôleurs d'accès, au détriment des prix, de la qualité, de la concurrence loyale, du choix et de l'innovation dans le secteur numérique.

(5)

Il s'ensuit que les processus du marché sont souvent incapables de garantir des résultats économiques équitables en ce qui concerne les services de plateforme essentiels. Si les articles 101 et 102 du traité sur le fonctionnement de l'Union européenne s'appliquent au comportement des contrôleurs d'accès, le champ d'application de ces dispositions se limite à certains cas de pouvoir de marché, par exemple la position dominante sur certains marchés et le comportement anticoncurrentiel, et l'application intervient ex post et requiert une enquête approfondie, au cas par cas, sur des faits souvent très complexes. En outre, le droit existant de l'Union ne répond pas, ou pas efficacement, aux entraves au bon fonctionnement du marché

intérieur dues au comportement de contrôleurs d'accès qui n'occupent pas nécessairement de position dominante au sens du droit de la concurrence.

(6)

En offrant des points d'accès à un grand nombre d'entreprises utilisatrices pour atteindre leurs utilisateurs finaux, partout dans l'Union et sur différents marchés, les contrôleurs d'accès ont un poids important sur le marché intérieur. L'incidence néfaste des pratiques déloyales sur le marché intérieur, et en particulier la faible contestabilité des services de plateforme essentiels, y compris les conséquences sociétales et économiques négatives de ces pratiques déloyales, a conduit les législateurs nationaux et les organismes de réglementation sectoriels à agir. Un certain nombre de solutions réglementaires ont déjà été adoptées au niveau national ou proposées en réponse aux questions liées aux pratiques déloyales et à la contestabilité des services numériques, ou à certaines d'entre elles au moins. Il en a résulté des divergences entre les solutions réglementaires, qui entraînent une fragmentation du marché intérieur, augmentant en conséquence le risque de voir croître les coûts de mise en conformité, en raison des différents dispositifs réglementaires nationaux.

(7)

Par conséquent, l'objectif du présent règlement est de contribuer au bon fonctionnement du marché intérieur en établissant des règles visant à garantir la contestabilité et l'équité des marchés dans le secteur numérique en général et pour les entreprises utilisatrices et les utilisateurs finaux des services de plateforme essentiels fournis par les contrôleurs d'accès en particulier. Les entreprises utilisatrices et les utilisateurs finaux de services de plateforme essentiels fournis par des contrôleurs d'accès devraient bénéficier de garanties réglementaires contre les pratiques déloyales des contrôleurs d'accès dans l'ensemble de l'Union, afin de faciliter les échanges transfrontières au sein de l'Union et, partant, le bon fonctionnement du marché intérieur, et d'éliminer la fragmentation existante ou éviter qu'elle apparaisse dans les domaines spécifiques régis par le présent règlement. De plus, si les contrôleurs d'accès adoptent généralement des modèles commerciaux et des structures algorithmiques mondiaux, ou du moins paneuropéens, ils peuvent adopter, et, dans certains cas, ont adopté, des conditions et pratiques commerciales différentes dans les divers États membres, qui sont susceptibles de créer des disparités entre les conditions de concurrence pour les utilisateurs de services de plateforme essentiels fournis par les contrôleurs d'accès, aux dépens de l'intégration du marché intérieur.

(8)

En rapprochant les législations nationales divergentes, il est possible d'éliminer les obstacles à la liberté de fournir et recevoir des services, y compris les services de vente au détail, au sein du marché intérieur. Un ensemble ciblé d'obligations légales harmonisées devrait par conséquent être établi à l'échelon de l'Union afin de garantir la contestabilité et l'équité des marchés numériques sur lesquels les contrôleurs d'accès opèrent au sein du marché intérieur, dans l'intérêt de l'économie de l'Union dans son ensemble et, en définitive, des consommateurs de l'Union.

(9)

Il n’est possible d’éviter effectivement une fragmentation du marché intérieur qu’en interdisant aux États membres d’appliquer des règles nationales qui relèvent du même champ d’application et poursuivent les mêmes objectifs que le présent règlement. Cela ne fait pas obstacle à la possibilité d’appliquer aux contrôleurs d’accès, au sens du présent règlement, d’autres règles nationales qui poursuivent d’autres objectifs d’intérêt public légitimes énoncés dans le traité sur le fonctionnement de l’Union européenne ou qui se justifient pour des raisons impérieuses d’intérêt général reconnues par la jurisprudence de la Cour de justice de l’Union européenne (ci-après dénommée «Cour de justice»).

(10)

Dans le même temps, puisque le présent règlement vise à compléter l’application du droit de la concurrence, il devrait s’appliquer, sans préjudice des articles 101 et 102 du traité sur le fonctionnement de l’Union européenne, aux règles de concurrence nationales correspondantes et aux autres règles de concurrence nationales relatives au comportement unilatéral, qui reposent sur une évaluation individualisée des positions et du comportement sur le marché, y compris les effets réels ou éventuels ainsi que la portée précise du comportement interdit, et qui prévoient la possibilité pour les entreprises de justifier objectivement le comportement en question par des motifs d’efficience, ainsi qu’aux règles nationales concernant le contrôle des concentrations. Toutefois, l’application de ces règles ne devrait pas porter atteinte aux obligations imposées aux contrôleurs d’accès au titre du présent règlement ni à leur application uniforme et effective sur le marché intérieur.

(11)

Les articles 101 et 102 du traité sur le fonctionnement de l’Union européenne et les règles de concurrence nationales correspondantes relatives aux comportements anticoncurrentiels multilatéraux et unilatéraux ainsi que le contrôle des concentrations ont pour objectif la protection d’une concurrence non faussée sur le marché. Le présent règlement poursuit un objectif complémentaire, mais différent de la protection d’une concurrence non faussée sur tout marché, au sens du droit de la concurrence, qui est de veiller à ce que les marchés sur lesquels les contrôleurs d’accès opèrent sont et restent contestables et équitables, indépendamment des effets réels, éventuels ou présumés sur la concurrence sur un marché donné du comportement d’un contrôleur d’accès couvert par ce règlement. Le présent règlement vise par conséquent à protéger un intérêt juridique différent de celui qui est protégé par lesdites règles et il devrait s’appliquer sans préjudice de leur application.

(12)

Le présent règlement devrait également s’appliquer sans préjudice des règles qui découlent d’autres actes du droit de l’Union régissant certains aspects de la fourniture de services couverts par le présent règlement, en particulier les règlements (UE) 2016/679 (4) et (UE) 2019/1150 (5) du Parlement européen et du Conseil et le règlement relatif à un marché intérieur des services numériques, les directives 2002/58/CE (6), 2005/29/CE (7), 2010/13/UE (8), (UE) 2015/2366 (9), (UE) 2019/790 (10) et (UE) 2019/882 (11) du Parlement européen et du Conseil et la directive 93/13/CEE du Conseil (12), ainsi que les règles nationales visant à mettre en œuvre ou à transposer ces actes juridiques de l’Union.

(13)

La faible contestabilité et les pratiques déloyales dans le secteur numérique sont plus fréquentes et prononcées pour certains services numériques que pour d'autres. C'est le cas en particulier pour les services numériques répandus et couramment utilisés, qui servent, pour la plupart, d'intermédiaires directs entre les entreprises utilisatrices et les utilisateurs finaux, et qui se caractérisent principalement par des économies d'échelle extrêmes, des effets de réseau très importants, la capacité de relier de nombreuses entreprises utilisatrices avec de nombreux utilisateurs finaux grâce au caractère multiface de ces services, des effets de verrouillage, l'absence de multihébergement ou l'intégration verticale. Il n'existe souvent qu'une seule grande entreprise ou très peu de grandes entreprises fournissant ces services numériques. Le plus souvent, ces entreprises sont devenues des contrôleurs d'accès pour les entreprises utilisatrices et les utilisateurs finaux, avec de profondes répercussions. En particulier, elles ont acquis la capacité de fixer facilement des conditions générales commerciales de manière unilatérale et préjudiciable pour leurs entreprises utilisatrices et utilisateurs finaux. Par conséquent, il est nécessaire de se concentrer uniquement sur les services numériques les plus largement utilisés par les entreprises utilisatrices et les utilisateurs finaux et pour lesquels les préoccupations relatives à la faible contestabilité et aux pratiques déloyales des contrôleurs d'accès sont plus apparentes et urgentes du point de vue du marché intérieur.

(14)

En particulier, les services d'intermédiation en ligne, les moteurs de recherche en ligne, les systèmes d'exploitation, les réseaux sociaux en ligne, les services de plateformes de partage de vidéos, les services de communications interpersonnelles non fondés sur la numérotation, les services d'informatique en nuage, les assistants virtuels, les navigateurs internet et les services de publicité en ligne, y compris les services d'intermédiation publicitaire, sont tous capables de toucher un grand nombre d'utilisateurs finaux comme d'entreprises, ce qui comporte un risque de pratiques commerciales déloyales. Ils devraient donc être inclus dans la définition des services de plateforme essentiels et relever du champ d'application du présent règlement. Les services d'intermédiation en ligne peuvent également opérer dans le domaine des services financiers, et ils peuvent agir en tant qu'intermédiaires ou être utilisés pour fournir des services tels que ceux énumérés de manière non exhaustive à l'annexe II de la directive (UE) 2015/1535 du Parlement européen et du Conseil (13). Aux fins du présent règlement, la définition des services de plateforme essentiels devrait être neutre sur le plan technologique et devrait s'entendre comme englobant ceux qui sont proposés par différents moyens ou sur différents dispositifs, tels que la télévision connectée ou les services numériques embarqués dans les véhicules. Dans certaines circonstances, la notion d'utilisateurs finaux devrait inclure les utilisateurs qui sont habituellement considérés comme des entreprises utilisatrices, mais qui, dans une situation donnée, n'utilisent pas les services de plateforme essentiels dans le but de fournir des biens ou des services à d'autres utilisateurs finaux, telles que, à titre d'exemple, les entreprises qui dépendent des services d'informatique en nuage pour leurs propres besoins.

(15)

Qu'un service numérique puisse être qualifié de service de plateforme essentiel ne suscite pas en soi de préoccupations suffisamment sérieuses en matière de contestabilité ou de pratiques déloyales. De telles préoccupations apparaissent seulement lorsqu'un service de plateforme essentiel constitue un point d'accès majeur et est exploité par une entreprise ayant un poids important sur le marché intérieur et jouissant d'une position solide et durable, ou par une entreprise susceptible de jouir d'une telle position dans un avenir proche. En conséquence,

l’ensemble ciblé de règles harmonisées prévues dans le présent règlement ne devrait s’appliquer qu’aux entreprises désignées sur la base de ces trois critères objectifs, et ne devrait s’appliquer qu’aux services de plateforme essentiels qui représentent, individuellement, un point d’accès majeur permettant aux entreprises utilisatrices d’atteindre les utilisateurs finaux. Le fait qu’une entreprise fournissant des services de plateforme essentiels puisse jouer un rôle d’intermédiaire non seulement entre les entreprises utilisatrices et les utilisateurs finaux, mais aussi entre utilisateurs finaux, par exemple dans le cas de services de communications interpersonnelles non fondés sur la numérotation, ne devrait pas empêcher de conclure qu’une telle entreprise constitue ou pourrait constituer un point d’accès majeur permettant aux entreprises utilisatrices d’atteindre des utilisateurs finaux.

(16)

Dans le but de garantir l’application effective du présent règlement aux entreprises fournissant des services de plateforme essentiels qui sont les plus susceptibles de remplir ces critères objectifs, et pour lesquels les pratiques déloyales affaiblissant la contestabilité sont les plus fréquentes et ont le plus de répercussions, la Commission devrait être en mesure de désigner directement comme contrôleurs d’accès les entreprises fournissant des services de plateforme essentiels qui répondent à certains seuils quantitatifs. Ces entreprises devraient en tout état de cause faire l’objet d’un processus de désignation rapide qui devrait commencer dès que le présent règlement devient applicable.

(17)

Le fait qu’une entreprise ait un chiffre d’affaires très élevé dans l’Union et fournisse un service de plateforme essentiel dans au moins trois États membres constitue un indice probant indiquant que cette entreprise a un impact significatif sur le marché intérieur. Il en va de même lorsqu’une entreprise fournissant un service de plateforme essentiel dans au moins trois États membres a une capitalisation boursière très importante ou une juste valeur marchande équivalente. Par conséquent, il convient que l’entreprise fournissant un service de plateforme essentiel soit présumée avoir un poids important sur le marché intérieur lorsqu’elle fournit ce service dans au moins trois États membres et lorsque soit le chiffre d’affaires de son groupe réalisé dans l’Union est égal ou supérieur à un seuil élevé spécifique, soit la capitalisation boursière de son groupe est égale ou supérieure à une valeur absolue élevée déterminée. En ce qui concerne les entreprises fournissant des services de plateforme essentiels appartenant à des entreprises qui ne sont pas cotées en Bourse, il convient de se référer à la juste valeur marchande équivalente. Il devrait être possible pour la Commission d’utiliser son pouvoir d’adopter des actes délégués afin de mettre au point une méthode objective pour calculer cette valeur.

Un chiffre d’affaires élevé du groupe, réalisé dans l’Union, associé au nombre seuil d’utilisateurs de services de plateforme essentiels dans l’Union témoigne d’une capacité relativement forte de monétiser ces utilisateurs. Une capitalisation boursière élevée par rapport au même nombre seuil d’utilisateurs dans l’Union traduit un potentiel relativement important de monétisation de ces utilisateurs dans un avenir proche. Ce potentiel de monétisation marque à son tour, en principe, la position de point d’accès des entreprises concernées. Ces deux indicateurs reflètent en outre la capacité financière des entreprises concernées, y compris leur faculté de tirer profit de leur accès aux marchés financiers dans le but de renforcer leur position. Cela peut notamment être le cas lorsque cet accès supérieur est utilisé pour acquérir d’autres entreprises, cette capacité s’étant à son tour avérée avoir des

répercussions néfastes potentielles sur l'innovation. La capitalisation boursière peut également refléter la position future attendue et les effets sur le marché intérieur des entreprises concernées, en dépit d'un chiffre d'affaires actuel potentiellement relativement faible. La valeur de la capitalisation boursière devrait reposer sur un niveau qui représente la capitalisation boursière moyenne des plus grandes entreprises cotées en Bourse de l'Union sur une période appropriée.

(18)

Alors qu'une capitalisation boursière égale ou supérieure au seuil au cours de l'exercice précédent devrait donner lieu à une présomption selon laquelle une entreprise fournissant des services de plateforme essentiels a un poids important sur le marché intérieur, une capitalisation boursière durable de l'entreprise fournissant des services de plateforme essentiels égale ou supérieure au seuil pendant trois ans ou plus devrait renforcer encore cette présomption.

(19)

En revanche, un certain nombre de facteurs relatifs à la capitalisation boursière pourraient nécessiter une évaluation approfondie pour déterminer s'il faut considérer qu'une entreprise fournissant des services de plateforme essentiels a un impact significatif sur le marché intérieur. Cela pourrait être le cas lorsque la capitalisation boursière de l'entreprise fournissant des services de plateforme essentiels au cours des exercices précédents était considérablement inférieure au seuil et que la volatilité de sa capitalisation boursière sur la période étudiée était disproportionnée par rapport à la volatilité globale du marché des actions, ou que sa trajectoire de capitalisation boursière par rapport aux tendances du marché était incompatible avec une croissance rapide et unidirectionnelle.

(20)

Disposer d'un nombre très important d'entreprises utilisatrices qui dépendent d'un service de plateforme essentiel pour atteindre un très grand nombre d'utilisateurs finaux actifs chaque mois permet à l'entreprise fournissant ce service d'exercer à son avantage une influence sur les activités d'une large part des entreprises utilisatrices et révèle, en principe, que cette entreprise est un point d'accès majeur. Il convient de fixer les niveaux respectifs pertinents de ces chiffres de manière à représenter un pourcentage substantiel de la population totale de l'Union en ce qui concerne les utilisateurs finaux et de la population totale des entreprises utilisant des services de plateforme essentiels pour déterminer le seuil relatif aux entreprises utilisatrices. Les utilisateurs finaux actifs et les entreprises utilisatrices actives devraient faire l'objet d'une identification et d'un calcul qui permettent de représenter correctement le rôle et la portée du service de plateforme essentiel spécifique en question. Afin d'apporter une sécurité juridique aux contrôleurs d'accès, les éléments permettant de déterminer le nombre d'utilisateurs finaux actifs et d'entreprises utilisatrices actives par service de plateforme essentiel devraient être énoncés dans une annexe du présent règlement. Les évolutions technologiques et autres peuvent avoir une influence sur ces éléments. Il convient dès lors d'habiliter la Commission à adopter des actes délégués pour modifier le présent règlement en actualisant la méthodologie et la liste d'indicateurs utilisés afin de déterminer le nombre d'utilisateurs finaux actifs et d'entreprises utilisatrices actives.

(21)

Une entreprise bénéficie ou bénéficiera probablement dans le futur d'une position solide et durable dans ses activités notamment lorsque la contestabilité de la position de l'entreprise fournissant le service de plateforme essentiel est limitée. Tel est probablement le cas si cette entreprise a fourni un service de plateforme essentiel dans au moins trois États membres à un très grand nombre d'entreprises utilisatrices et d'utilisateurs finaux pendant une période d'au moins trois ans.

(22)

Les évolutions du marché et de la technologie peuvent influer sur de tels seuils. La Commission devrait donc être habilitée à adopter des actes délégués visant à préciser la méthode utilisée pour déterminer si les seuils quantitatifs sont atteints, et à l'adapter régulièrement aux évolutions du marché et de la technologie, le cas échéant. Ces actes délégués ne devraient pas modifier les seuils quantitatifs fixés dans le présent règlement.

(23)

Une entreprise fournissant des services de plateforme essentiels devrait pouvoir, dans des circonstances exceptionnelles, renverser la présomption selon laquelle elle a un poids important sur le marché intérieur en démontrant que, même si elle atteint les seuils quantitatifs fixés dans le présent règlement, elle ne remplit pas les exigences nécessaires pour être désignée comme contrôleur d'accès. La charge de la preuve que la présomption découlant du respect de seuils quantitatifs ne devrait pas s'appliquer incombe à cette entreprise. La Commission ne devrait prendre en considération, dans son évaluation des preuves et des arguments présentés, que les éléments directement liés aux critères quantitatifs, à savoir le poids de l'entreprise fournissant des services de plateforme essentiels sur le marché intérieur, au-delà des recettes ou de la capitalisation boursière, par exemple sa taille en termes absolus ainsi que le nombre d'États membres dans lesquels elle est présente; la mesure dans laquelle le nombre d'entreprises utilisatrices et d'utilisateurs finaux réels dépasse les seuils ainsi que l'importance du service de plateforme essentiel de l'entreprise, compte tenu de l'échelle globale des activités du service de plateforme essentiel concerné; et le nombre d'années pendant lesquelles les seuils ont été atteints.

Toute justification reposant sur des motifs économiques, en rapport avec la définition du marché ou visant à démontrer des gains d'efficience découlant d'un type particulier de comportement de l'entreprise fournissant des services de plateforme essentiels, devrait être rejetée, car elle n'est pas pertinente pour la désignation d'un contrôleur d'accès. Si les arguments présentés ne sont pas suffisamment étayés et ne remettent manifestement pas en cause la présomption, la Commission devrait pouvoir les rejeter dans le délai de 45 jours ouvrables prévu pour la désignation. La Commission devrait être en mesure de prendre une décision en se fondant sur les informations disponibles en ce qui concerne les seuils quantitatifs lorsque l'entreprise fournissant les services de plateforme essentiels entrave l'enquête de manière significative en ne se conformant pas aux mesures d'enquête prises par la Commission.

(24)

Il convient également de prévoir l'évaluation du rôle de contrôleur d'accès que jouent les entreprises fournissant des services de plateforme essentiels qui n'atteignent pas tous les

seuils quantitatifs, à la lumière des exigences objectives globales selon lesquelles elles ont un poids important sur le marché intérieur, servent de points d'accès majeurs permettant aux entreprises utilisatrices d'atteindre les utilisateurs finaux et bénéficient d'une position solide et durable dans leurs activités, ou sont susceptibles d'en bénéficier dans un avenir proche. Lorsque l'entreprise qui fournit des services de plateforme essentiels est une moyenne, une petite ou une microentreprise, l'évaluation devrait soigneusement examiner si une telle entreprise serait en mesure de compromettre substantiellement la contestabilité des services de plateforme essentiels, étant donné que le présent règlement vise principalement les grandes entreprises disposant d'un pouvoir économique considérable plutôt que les moyennes, les petites ou les microentreprises.

(25)

Une telle évaluation ne peut être effectuée qu'à la lumière d'une enquête de marché, tout en tenant compte des seuils quantitatifs. Dans son évaluation, la Commission devrait prendre en compte les objectifs consistant à préserver et à promouvoir l'innovation et la qualité des produits et services numériques ainsi que l'équité et la compétitivité des prix, et veiller à ce que les niveaux de qualité et de choix offerts aux entreprises utilisatrices et aux utilisateurs finaux soient ou restent élevés. Des éléments spécifiques aux entreprises fournissant des services de plateforme essentiels concernées peuvent être pris en considération, tels que des économies d'échelle ou de gamme extrêmes, des effets de réseau très importants, des avantages fondés sur les données, leur capacité de relier de nombreuses entreprises utilisatrices avec de nombreux utilisateurs finaux grâce à leur caractère multiface, les effets de verrouillage, l'absence de multihébergement, une structure d'entreprise conglomérale ou l'intégration verticale. En outre, une capitalisation boursière très importante, un ratio de valeur de fonds propres par rapport au bénéfice très élevé ou un chiffre d'affaires très important tiré des utilisateurs finaux d'un seul service de plateforme essentiel peuvent être utilisés comme indicateurs du potentiel d'utilisation d'un effet de levier par ces entreprises et du basculement du marché en leur faveur. Avec la capitalisation boursière, les taux de croissance relatifs élevés sont des exemples de paramètres dynamiques particulièrement pertinents pour identifier les entreprises fournissant des services de plateforme essentiels dont on peut prévoir qu'elles acquerront une position solide et durable. La Commission devrait être en mesure de prendre une décision en tirant des conclusions défavorables à partir des données disponibles lorsque l'entreprise fournissant des services de plateforme essentiels entrave l'enquête de manière significative en refusant de se conformer aux mesures d'enquête prises par la Commission.

(26)

Un sous-ensemble de règles particulier devrait s'appliquer aux entreprises fournissant des services de plateforme essentiels dont on peut prévoir qu'elles bénéficieront d'une position solide et durable dans un avenir proche. Les mêmes caractéristiques spécifiques des services de plateforme essentiels les rendent susceptibles de basculer: dès qu'une entreprise fournissant le service de plateforme essentiel a obtenu un certain avantage par rapport à ses concurrentes ou à des concurrentes potentielles en termes de taille ou de pouvoir d'intermédiation, sa position pourrait devenir inattaquable et évoluer au point de devenir solide et durable dans un avenir proche. Les entreprises peuvent tenter de provoquer ce basculement et devenir des contrôleurs d'accès en recourant à certaines des conditions et pratiques déloyales régies par le présent règlement. Il semble adéquat d'intervenir dans une telle situation, avant que le marché ne bascule de manière irréversible.

(27)

Cependant, une telle intervention précoce devrait se limiter à imposer uniquement les obligations nécessaires et appropriées pour veiller à ce que les services concernés restent contestables et permettre que le risque qualifié de conditions et pratiques déloyales soit évité. Les obligations empêchant l'entreprise fournissant des services de plateforme essentiels concernée de bénéficier d'une position solide et durable dans ses activités, telles que les obligations visant à empêcher l'utilisation d'un effet de levier et celles facilitant le changement de plateforme et le multihébergement, visent plus directement cet objectif. Dans le but de garantir la proportionnalité, la Commission devrait également appliquer, parmi ce sous-ensemble d'obligations, uniquement celles qui sont nécessaires et proportionnées pour atteindre les objectifs du présent règlement, et devrait régulièrement réexaminer ces obligations afin de déterminer si elles doivent être maintenues, supprimées ou adaptées.

(28)

Appliquer uniquement les obligations qui sont nécessaires et proportionnées pour atteindre les objectifs du présent règlement devrait permettre à la Commission d'intervenir efficacement et en temps opportun, tout en respectant pleinement la proportionnalité des mesures envisagées. Cela devrait en outre rassurer les acteurs actuels ou potentiels du marché quant à la contestabilité et à l'équité des services visés.

(29)

Les contrôleurs d'accès devraient respecter les obligations énoncées dans le présent règlement en ce qui concerne chacun des services de plateforme essentiels énumérés dans la décision de désignation correspondante. Le cas échéant, les obligations devraient s'appliquer tout en tenant compte de la situation de conglomérat des contrôleurs d'accès. En outre, la Commission devrait pouvoir, par voie de décision, imposer des mesures d'exécution au contrôleur d'accès. Ces mesures d'exécution devraient être conçues efficacement, eu égard aux caractéristiques des services de plateforme essentiels ainsi qu'aux risques éventuels de contournement, et dans le respect du principe de proportionnalité et des droits fondamentaux des entreprises visées et des tiers.

(30)

La nature technologique complexe et en très rapide évolution des services de plateforme essentiels nécessite un réexamen régulier du statut des contrôleurs d'accès, y compris ceux dont on peut prévoir qu'ils bénéficieront, dans un avenir proche, d'une position solide et durable dans leurs activités. Afin de fournir à tous les acteurs du marché, y compris les contrôleurs d'accès, la sécurité requise en ce qui concerne les obligations juridiques applicables, il convient de fixer un délai pour ces réexamens réguliers. Il importe également de mener ces réexamens à intervalles réguliers et au moins tous les trois ans. En outre, il importe de préciser que tout changement des éléments de fait sur la base desquels une entreprise fournissant des services de plateforme essentiels a été désignée comme contrôleur d'accès ne devrait pas nécessiter que la décision de désignation soit modifiée. Une modification ne sera nécessaire que si le changement des éléments de fait entraîne également une modification de l'évaluation. Pour décider s'il en va ainsi ou pas, il convient de se fonder sur une évaluation au cas par cas des faits et circonstances.

(31)

Pour préserver la contestabilité et l'équité des services de plateforme essentiels fournis par les contrôleurs d'accès, il est important de prévoir de manière claire et non équivoque un ensemble de règles harmonisées relatives à ces services. De telles règles sont nécessaires face au risque que représentent les effets néfastes des pratiques des contrôleurs d'accès, et sont bénéfiques pour l'environnement commercial des services concernés, les utilisateurs et, en fin de compte, la société dans son ensemble. Les obligations correspondent aux pratiques qui sont considérées comme compromettant la contestabilité ou comme déloyales, ou les deux, compte tenu des caractéristiques du secteur numérique, et qui ont une incidence directe particulièrement négative sur les entreprises utilisatrices et les utilisateurs finaux. Les obligations énoncées dans le présent règlement devraient pouvoir prendre spécifiquement en considération la nature des services de plateforme essentiels fournis. Les obligations prévues par le présent règlement devraient non seulement garantir la contestabilité et l'équité en ce qui concerne les services de plateforme essentiels énumérés dans la décision de désignation, mais aussi en ce qui concerne d'autres produits et services numériques grâce auxquels les contrôleurs d'accès tirent parti de leur position de point d'accès et qui sont souvent fournis en accompagnement ou à l'appui des services de plateforme essentiels.

(32)

Aux fins du présent règlement, la contestabilité devrait se rapporter à la capacité des entreprises à surmonter efficacement les barrières à l'entrée et à l'expansion, et à faire concurrence au contrôleur d'accès sur la base des mérites de leurs produits et services. Les caractéristiques des services de plateforme essentiels dans le secteur numérique, telles que les effets de réseau, les importantes économies d'échelle et les avantages tirés des données, limitent la contestabilité de ces services et des écosystèmes connexes. Cette faible contestabilité réduit les incitations à innover et à améliorer les produits et services pour le contrôleur d'accès, ses entreprises utilisatrices, ses concurrents et ses clients, et a donc une incidence négative sur le potentiel d'innovation de l'économie des plateformes en ligne au sens large. La contestabilité des services dans le secteur numérique peut également être limitée s'il y a plus d'un contrôleur d'accès pour un service de plateforme essentiel. Le présent règlement devrait donc interdire certaines pratiques des contrôleurs d'accès qui sont susceptibles de renforcer les barrières à l'entrée ou à l'expansion, et imposer aux contrôleurs d'accès certaines obligations qui tendent à abaisser ces barrières. Les obligations devraient également porter sur les situations dans lesquelles la position du contrôleur d'accès peut être tellement solide que la concurrence interplateformes n'est pas effective à court terme, ce qui signifie que la concurrence interplateformes doit être créée ou renforcée.

(33)

Aux fins du présent règlement, l'iniquité devrait être liée à un déséquilibre entre les droits et obligations des entreprises utilisatrices lorsque le contrôleur d'accès obtient un avantage disproportionné. Les acteurs du marché, y compris les entreprises utilisatrices de services de plateforme essentiels et les autres fournisseurs de services fournis en accompagnement ou à l'appui de ces services de plateforme essentiels, devraient être en mesure de tirer adéquatement parti des avantages découlant de leurs efforts d'innovation ou autres. En raison de leur position de point d'accès et de leur pouvoir de négociation supérieur, il se peut que les contrôleurs d'accès aient des comportements qui ne permettent pas à d'autres de tirer

pleinement parti des avantages de leurs propres contributions et qu'ils fixent unilatéralement des conditions déséquilibrées pour l'utilisation de leurs services de plateforme essentiels ou des services fournis en accompagnement ou à l'appui de leurs services de plateforme essentiels. Ce déséquilibre n'est pas exclu du simple fait que le contrôleur d'accès offre gratuitement un service particulier à un groupe spécifique d'utilisateurs, et il peut également consister à écarter ou à défavoriser les entreprises utilisatrices, en particulier si ces dernières sont en concurrence avec les services fournis par le contrôleur d'accès. Le présent règlement devrait donc imposer des obligations aux contrôleurs d'accès pour ce qui est de ce type de comportements.

(34)

La contestabilité et l'équité sont étroitement liées. L'absence de contestabilité ou la faible contestabilité d'un service donné peut permettre à un contrôleur d'accès de se livrer à des pratiques déloyales. De même, les pratiques déloyales d'un contrôleur d'accès peuvent réduire la possibilité pour les entreprises utilisatrices ou autres de contester sa position. Une obligation spécifique prévue par le présent règlement peut donc porter sur ces deux éléments.

(35)

Dans la mesure où il n'existe pas de mesures alternatives moins restrictives qui conduiraient au même résultat, eu égard au besoin de protéger l'ordre public et la vie privée, et de lutter contre les pratiques commerciales frauduleuses et trompeuses, les obligations énoncées dans le présent règlement sont donc nécessaires pour répondre aux questions d'intérêt général soulevées.

(36)

Les contrôleurs d'accès collectent souvent directement les données à caractère personnel des utilisateurs finaux aux fins de la fourniture de services de publicité en ligne lorsque les utilisateurs finaux utilisent des sites internet et des applications logicielles de tiers. Les tiers fournissent en outre aux contrôleurs d'accès les données à caractère personnel de leurs utilisateurs finaux aux fins de l'utilisation de certains services fournis par les contrôleurs d'accès dans le cadre de leurs services de plateforme essentiels, par exemple des audiences personnalisées. Le traitement, aux fins de la fourniture de services de publicité en ligne, de données à caractère personnel de tiers utilisant des services de plateforme essentiels offre aux contrôleurs d'accès des avantages potentiels en ce qui concerne l'accumulation de données, érigeant de ce fait des barrières à l'entrée. En effet, les contrôleurs d'accès traitent des données à caractère personnel d'un nombre nettement plus élevé de tiers que d'autres entreprises. Des avantages similaires résultent des pratiques consistant i) à combiner les données à caractère personnel des utilisateurs finaux collectées auprès d'un service de plateforme essentiel avec les données collectées auprès d'autres services, ii) à recourir à l'utilisation croisée de données à caractère personnel provenant d'un service de plateforme essentiel dans d'autres services proposés séparément par le contrôleur d'accès, notamment ceux qui ne sont pas fournis en accompagnement ou à l'appui du service de plateforme essentiel concerné, et vice versa, ou iii) à connecter des utilisateurs finaux à différents services de contrôleurs d'accès afin de combiner des données à caractère personnel. Afin d'éviter que la contestabilité des services de plateforme essentiels ne soit injustement compromise par les contrôleurs d'accès, ceux-ci devraient permettre aux utilisateurs finaux de choisir librement d'adhérer à de telles pratiques de traitement de données et de connexion en

proposant une autre possibilité moins personnalisée, mais équivalente, et sans subordonner l'utilisation du service de plateforme essentiel ou certaines de ses fonctionnalités au consentement de l'utilisateur final. Cela devrait être sans préjudice du fait que le contrôleur d'accès traite des données à caractère personnel ou connecte des utilisateurs finaux à un service, en invoquant comme base juridique l'article 6, paragraphe 1, points c), d) et e), du règlement (UE) 2016/679, mais pas l'article 6, paragraphe 1, points b) et f), dudit règlement.

(37)

L'autre possibilité moins personnalisée ne devrait pas être différente ou de qualité moindre par rapport au service offert aux utilisateurs finaux qui donnent leur consentement, sauf si une baisse de la qualité résulte directement du fait que le contrôleur d'accès n'est pas en mesure de traiter ces données à caractère personnel ou de connecter les utilisateurs finaux à un service. Il ne devrait pas être plus difficile de ne pas donner son consentement que de le donner. Lorsque le contrôleur d'accès demande le consentement, il devrait prendre les devants et présenter une solution conviviale à l'utilisateur final pour que celui-ci puisse donner, modifier ou retirer son consentement de façon explicite, claire et simple. En particulier, le consentement devrait être donné par une déclaration ou un acte positif clair par lequel l'utilisateur final manifeste de façon libre, spécifique, éclairée et univoque son accord, au sens du règlement (UE) 2016/679. Au moment de donner son consentement, et uniquement lorsqu'il y a lieu, l'utilisateur final devrait être informé que le fait de ne pas donner son consentement peut se traduire par une offre moins personnalisée, mais que, à tous autres égards, le service de plateforme essentiel restera inchangé et qu'aucune fonctionnalité ne sera supprimée. À titre exceptionnel, si le consentement ne peut être donné directement au service de plateforme essentiel du contrôleur d'accès, les utilisateurs finaux devraient être en mesure de donner leur consentement par l'intermédiaire de chaque service tiers qui utilise ce service de plateforme essentiel, pour permettre au contrôleur d'accès de traiter des données à caractère personnel aux fins de la fourniture de services de publicité en ligne.

Enfin, il devrait être aussi simple de retirer son consentement que de le donner. Les contrôleurs d'accès ne devraient pas concevoir, organiser ou exploiter leurs interfaces en ligne de façon à tromper ou à manipuler les utilisateurs finaux ou, de toute autre manière, à altérer ou à limiter substantiellement la capacité des utilisateurs finaux de donner librement leur consentement. En particulier, les contrôleurs d'accès ne devraient pas être autorisés à demander plus d'une fois par an aux utilisateurs finaux de donner leur consentement pour une finalité de traitement identique à celle pour laquelle ils n'ont initialement pas donné leur consentement ou ont retiré leur consentement. Le présent règlement est sans préjudice du règlement (UE) 2016/679, y compris son cadre d'application, qui reste pleinement applicable en ce qui concerne toute réclamation introduite par des personnes concernées en rapport avec une infraction aux droits que leur confère ledit règlement.

(38)

Les enfants méritent une protection spécifique en ce qui concerne leurs données à caractère personnel, notamment pour ce qui est de l'utilisation de leurs données à caractère personnel à des fins de communication commerciale ou de création de profils d'utilisateurs. La protection des enfants en ligne est un objectif important de l'Union, qui devrait être pris en compte dans le droit applicable de l'Union. Dans ce contexte, il convient de prendre dûment en considération le règlement relatif au marché intérieur des services numériques. Aucune

disposition du présent règlement ne dispense les contrôleurs d'accès de l'obligation de protéger les enfants prévue dans le droit applicable de l'Union.

(39)

Dans certains cas, par exemple lorsqu'ils imposent des conditions contractuelles, les contrôleurs d'accès peuvent restreindre la capacité des entreprises utilisatrices de leurs services d'intermédiation en ligne de proposer des produits ou des services aux utilisateurs finaux à des conditions plus favorables, notamment en matière de prix, par le biais d'autres services d'intermédiation en ligne ou de canaux de vente directe en ligne. Lorsque de telles restrictions concernent des services d'intermédiation en ligne de tiers, elles limitent la contestabilité interplateformes, et donc le choix des utilisateurs finaux pour ce qui est des autres services d'intermédiation en ligne. Lorsque ces restrictions concernent des canaux de vente directe en ligne, elles limitent injustement la liberté des entreprises utilisatrices d'utiliser ces canaux. Pour que les entreprises utilisatrices des services d'intermédiation en ligne des contrôleurs d'accès puissent librement choisir d'autres services d'intermédiation en ligne ou d'autres canaux de vente directe en ligne, et différencier les conditions dans lesquelles elles proposent leurs produits ou services aux utilisateurs finaux, les contrôleurs d'accès ne devraient pas être autorisés à limiter les entreprises utilisatrices dans leur choix de différencier les conditions commerciales, y compris les prix. Une telle restriction devrait s'appliquer à toute mesure dont les effets sont équivalents, telle que l'augmentation des taux de commission ou le déréférencement des offres des entreprises utilisatrices.

(40)

Afin d'éviter une aggravation de leur dépendance à l'égard des services de plateforme essentiels des contrôleurs d'accès et de promouvoir le multihébergement, les entreprises utilisatrices de ces contrôleurs d'accès devraient être libres de promouvoir et de choisir le canal de distribution qu'elles jugent le plus approprié pour interagir avec les utilisateurs finaux qu'elles ont déjà acquis par l'intermédiaire des services de plateforme essentiels fournis par les contrôleurs d'accès ou d'autres canaux. Cela devrait être valable pour la promotion des offres, y compris au moyen d'une application logicielle de l'entreprise utilisatrice, ainsi que pour toute forme de communication et de conclusion de contrats entre les entreprises utilisatrices et les utilisateurs finaux. Un utilisateur final est un utilisateur final acquis s'il a déjà établi une relation commerciale avec l'entreprise utilisatrice et que, le cas échéant, le contrôleur d'accès a été rémunéré directement ou indirectement par l'entreprise utilisatrice pour faciliter l'acquisition initiale de l'utilisateur final par l'entreprise utilisatrice. De telles relations commerciales peuvent être payantes ou gratuites, par exemple, des essais gratuits, des niveaux de service gratuits, et peuvent avoir été établies soit via le service de plateforme essentiel du contrôleur d'accès, soit par tout autre canal. Inversement, les utilisateurs finaux devraient également être libres de choisir les offres de ces entreprises utilisatrices et de conclure des contrats avec elles, soit, le cas échéant, par l'intermédiaire des services de plateforme essentiels du contrôleur d'accès, soit à partir d'un canal de distribution direct de l'entreprise utilisatrice ou d'un autre canal indirect auquel l'entreprise utilisatrice a recours.

(41)

La capacité des utilisateurs finaux d'acheter du contenu, des abonnements, des fonctionnalités ou autres en dehors des services de plateforme essentiels des contrôleurs d'accès ne devrait

être ni compromise ni restreinte. Il convient particulièrement d'éviter une situation dans laquelle les contrôleurs d'accès restreignent l'utilisation de ces services et l'accès à ces services par les utilisateurs finaux au moyen d'une application logicielle fonctionnant sur leur service de plateforme essentiel. Par exemple, les abonnés à un contenu en ligne acheté sans passer par une application logicielle, une boutique d'applications logicielles ou un assistant virtuel ne devraient pas être empêchés d'accéder à ce contenu en ligne sur une application logicielle du service de plateforme essentiel du contrôleur d'accès au seul motif que l'achat s'est fait sans passer par cette application logicielle, cette boutique d'applications logicielles ou cet assistant virtuel.

(42)

Garantir le droit des entreprises utilisatrices et utilisateurs finaux, y compris les lanceurs d'alerte, de faire part de préoccupations quant aux pratiques déloyales des contrôleurs d'accès en signalant tout problème lié au non-respect du droit de l'Union ou national pertinent à toute autorité administrative ou autre autorité publique compétente, y compris les juridictions nationales, est essentiel à la préservation d'un environnement commercial équitable et à la protection de la contestabilité du secteur numérique. Par exemple, il se peut que des entreprises utilisatrices ou des utilisateurs finaux veuillent se plaindre de différents types de pratiques déloyales, tels que des conditions d'accès discriminatoires, la clôture injustifiée de comptes d'entreprises utilisatrices ou la motivation peu claire de déréférencements de produits. Par conséquent, toute pratique qui constituerait un obstacle pour ces utilisateurs ou qui les empêcherait de quelque manière que ce soit de faire part de leurs préoccupations ou de demander réparation, au moyen par exemple de clauses de confidentialité dans les accords ou d'autres conditions écrites, devrait être interdite. Cette interdiction devrait être sans préjudice du droit des entreprises utilisatrices et des contrôleurs d'accès d'établir, dans leurs accords, les conditions d'utilisation, y compris le recours à des mécanismes légaux de traitement des plaintes, notamment à tout mécanisme de règlement extrajudiciaire des litiges, ou le recours à la compétence de tribunaux spécifiques dans le respect du droit de l'Union et du droit national applicable. Cela devrait également être sans préjudice du rôle que jouent les contrôleurs d'accès dans la lutte contre la présence de contenus illicites en ligne.

(43)

Certains services fournis en accompagnement ou à l'appui des services de plateforme essentiels pertinents du contrôleur d'accès, par exemple les services d'identification, les moteurs de navigateurs internet, les services de paiement ou les services techniques qui soutiennent la fourniture de services de paiement, tels que les systèmes de paiement pour les achats intégrés dans des applications, sont essentiels pour que les entreprises utilisatrices puissent mener leurs activités et pour leur permettre d'optimiser leurs services. En particulier, chaque navigateur est construit sur un moteur de navigateur internet, qui est responsable des principales fonctionnalités du navigateur, telles que la vitesse, la fiabilité et la compatibilité internet. Lorsque les contrôleurs d'accès exploitent et imposent des moteurs de navigateurs internet, ils sont en mesure de déterminer quelles fonctionnalités et quelles normes s'appliqueront non seulement à leurs propres navigateurs internet, mais aussi aux navigateurs internet concurrents et, en aval, aux applications logicielles internet. Les contrôleurs d'accès ne devraient donc pas tirer parti de leur position pour exiger des entreprises utilisatrices qui dépendent d'eux qu'elles recourent à l'un quelconque des services fournis en accompagnement ou à l'appui des services de plateforme essentiels par le contrôleur d'accès lui-même dans le cadre de la fourniture de services ou de produits par ces entreprises

utilisatrices. Pour éviter une situation dans laquelle les contrôleurs d'accès imposent indirectement aux entreprises utilisatrices leurs propres services fournis en accompagnement ou à l'appui des services de plateforme essentiels, il devrait en outre être interdit aux contrôleurs d'accès d'exiger des utilisateurs finaux qu'ils recourent à ces services lorsque cette exigence serait imposée dans le contexte du service fourni aux utilisateurs finaux par l'entreprise utilisatrice qui recourt au service de plateforme essentiel du contrôleur d'accès. Cette interdiction vise à protéger la liberté de l'entreprise utilisatrice de choisir d'autres services que ceux du contrôleur d'accès et ne devrait pas être interprétée comme obligeant l'entreprise utilisatrice à proposer de telles alternatives à ses utilisateurs finaux.

(44)

Le procédé consistant à exiger des entreprises utilisatrices ou des utilisateurs finaux qu'ils s'abonnent ou s'enregistrent auprès de tout autre service de plateforme essentiel d'un contrôleur d'accès énuméré dans la décision de désignation ou qu'ils atteignent les seuils quantitatifs concernant les utilisateurs finaux actifs et les entreprises utilisatrices actives fixés dans le présent règlement, comme condition d'utilisation, d'accès, d'inscription ou d'enregistrement pour un service de plateforme essentiel, donne aux contrôleurs d'accès un moyen de capter ou de rendre captifs de nouvelles entreprises utilisatrices et de nouveaux utilisateurs finaux pour ses services de plateforme essentiels en faisant en sorte que les entreprises utilisatrices ne puissent accéder à un service de plateforme essentiel sans s'enregistrer ou créer un compte dans le but de recevoir un deuxième service de plateforme essentiel. Ce procédé confère également aux contrôleurs d'accès un avantage potentiel en ce qui concerne l'accumulation de données. En tant que tel, il est donc susceptible d'ériger des barrières à l'entrée et devrait être interdit.

(45)

Les conditions dans lesquelles les contrôleurs d'accès fournissent des services de publicité en ligne aux entreprises utilisatrices, dont les annonceurs et les éditeurs, manquent souvent de transparence et sont opaques. Cette opacité est en partie liée aux pratiques de quelques plateformes, mais elle résulte aussi de la complexité même de la publicité programmatique moderne. On estime que ce secteur est devenu moins transparent après l'introduction de la nouvelle législation portant sur la vie privée. Pour les annonceurs et les éditeurs, cela conduit souvent à un manque d'informations et de connaissances quant aux conditions des services de publicité en ligne qu'ils achètent et compromet leur capacité à changer d'entreprise fournissant des services de publicité en ligne. En outre, les coûts des services de publicité en ligne dans ces conditions sont susceptibles d'être plus élevés que dans un environnement de plateforme plus équitable, plus transparent et contestable. Ces coûts plus élevés se répercuteront vraisemblablement sur les prix que paieront les utilisateurs finaux pour de nombreux produits et services quotidiens qui reposent sur l'utilisation des services de publicité en ligne. Les obligations de transparence devraient donc exiger des contrôleurs d'accès qu'ils communiquent gratuitement aux annonceurs et éditeurs à qui ils fournissent des services de publicité en ligne, sur demande, les informations nécessaires aux deux parties pour comprendre le prix payé pour chacun des différents services de publicité en ligne fournis dans le cadre de la chaîne de valeur publicitaire correspondante.

Ces informations devraient être fournies, sur demande, à un annonceur au niveau d'une publicité individuelle en ce qui concerne le prix et les honoraires facturés à cet annonceur et, sous réserve de l'accord de l'éditeur propriétaire de l'inventaire dans lequel la publicité est

affichée, la rémunération perçue par cet éditeur consentant. La fourniture quotidienne de ces informations permettra aux annonceurs de recevoir des informations présentant un niveau de granularité suffisant pour comparer les coûts d'utilisation des services de publicité en ligne des contrôleurs d'accès aux coûts liés à l'utilisation des services de publicité en ligne d'autres entreprises. Si certains éditeurs ne donnent pas leur consentement au partage des informations pertinentes avec l'annonceur, le contrôleur d'accès devrait fournir à l'annonceur les informations relatives à la rémunération moyenne journalière perçue par ces éditeurs pour les publicités concernées. La même obligation et les mêmes principes de partage des informations pertinentes concernant la fourniture de services de publicité en ligne devraient s'appliquer aux demandes des éditeurs. Étant donné que les contrôleurs d'accès peuvent utiliser différents modèles de tarification pour la fourniture de services de publicité en ligne aux annonceurs et aux éditeurs, par exemple un prix par impression, par vue ou tout autre critère, les contrôleurs d'accès devraient également indiquer la méthode de calcul de chacun des prix et de chacune des rémunérations.

(46)

Dans certaines circonstances, un contrôleur d'accès joue un double rôle lorsque, en tant qu'entreprise fournissant des services de plateforme essentiels, il fournit à ses entreprises utilisatrices un service de plateforme essentiel et éventuellement d'autres services fournis en accompagnement ou à l'appui de ce service de plateforme essentiel, et que, parallèlement, il se trouve ou compte se trouver en concurrence avec ces mêmes entreprises pour la fourniture aux mêmes utilisateurs finaux de services ou de produits identiques ou similaires. Dans de telles circonstances, un contrôleur d'accès peut profiter de son double rôle pour utiliser des données générées ou fournies par ses entreprises utilisatrices dans le cadre des activités qu'elles exercent lorsqu'elles ont recours aux services de plateforme essentiels ou aux services fournis en accompagnement ou à l'appui de ces services de plateforme essentiels, aux fins de ses propres services ou produits. Les données de l'entreprise utilisatrice peuvent également inclure toutes données générées par les activités de ses utilisateurs finaux ou fournies au cours de ces activités. Tel peut être le cas lorsqu'un contrôleur d'accès fournit aux entreprises utilisatrices une place de marché en ligne ou une boutique d'applications logicielles, et que, parallèlement, il fournit des services en tant qu'entreprise fournissant des services de détail en ligne ou des applications logicielles. Afin d'empêcher les contrôleurs d'accès de tirer injustement profit de leur double rôle, il est nécessaire de veiller à ce qu'ils n'utilisent pas les données agrégées ou non agrégées, qui pourraient comprendre les données anonymisées et les données à caractère personnel qui ne sont pas accessibles au grand public, dans le but de fournir des services similaires à ceux de leurs entreprises utilisatrices. Cette obligation devrait s'appliquer au contrôleur d'accès dans son ensemble, et notamment mais pas exclusivement, à son unité opérationnelle qui est en concurrence avec les entreprises utilisatrices d'un service de plateforme essentiel.

(47)

Les entreprises utilisatrices peuvent également acheter des services de publicité en ligne à une entreprise fournissant des services de plateforme essentiels dans le but de fournir des biens et des services aux utilisateurs finaux. Dans ces circonstances, il peut arriver que les données ne soient pas générées dans le service de plateforme essentiel, mais soient fournies à ce service par l'entreprise utilisatrice, ou soient générées à partir des opérations qu'elle effectue par l'intermédiaire du service de plateforme essentiel concerné. Dans certains cas, ce service de plateforme essentiel fournissant de la publicité peut jouer un double rôle en tant qu'entreprise

fournissant des services de publicité en ligne et en tant qu'entreprise fournissant des services entrant en concurrence avec ceux des entreprises utilisatrices. En conséquence, l'interdiction imposée à un contrôleur d'accès jouant un double rôle d'utiliser les données des entreprises utilisatrices devrait également s'appliquer aux données qu'un service de plateforme essentiel a reçues des entreprises aux fins de la fourniture de services de publicité en ligne liés à ce service de plateforme essentiel.

(48)

En ce qui concerne les services d'informatique en nuage, l'obligation de ne pas utiliser les données des entreprises utilisatrices devrait s'étendre aux données fournies ou générées par les entreprises utilisatrices dans le cadre de leur utilisation du service d'informatique en nuage du contrôleur d'accès, ou par l'intermédiaire de sa boutique d'applications logicielles qui permet aux utilisateurs finaux des services d'informatique en nuage d'accéder aux applications logicielles. Cette obligation ne devrait pas porter atteinte au droit du contrôleur d'accès d'utiliser des données agrégées pour la fourniture d'autres services fournis en accompagnement ou à l'appui de son service de plateforme essentiel, par exemple des services d'analyse de données, dans le respect du règlement (UE) 2016/679 et de la directive 2002/58/CE, ainsi que des obligations pertinentes du présent règlement relatives à ces services.

(49)

Un contrôleur d'accès peut recourir à divers moyens pour favoriser ses propres services ou produits ou ceux d'un tiers sur son système d'exploitation, son assistant virtuel ou son navigateur internet au détriment de services identiques ou similaires que les utilisateurs finaux pourraient obtenir par l'intermédiaire d'autres tiers. Cela peut notamment se produire lorsque certaines applications logicielles ou certains services sont préinstallés par le contrôleur d'accès. Pour permettre aux utilisateurs finaux de choisir, les contrôleurs d'accès ne devraient pas les empêcher de désinstaller toute application logicielle sur leur système d'exploitation. Il ne devrait être possible pour le contrôleur d'accès de restreindre cette désinstallation que lorsque ces applications logicielles sont essentielles au fonctionnement du système d'exploitation ou de l'appareil. Les contrôleurs d'accès devraient par ailleurs permettre aux utilisateurs finaux de modifier facilement les paramètres par défaut du système d'exploitation, de l'assistant virtuel et du navigateur internet lorsque ces paramètres par défaut favorisent leurs propres applications logicielles et services. Cela peut se faire notamment en présentant un choix à l'écran, lorsque l'utilisateur recourt pour la première fois à un moteur de recherche en ligne, à un assistant virtuel ou à un navigateur internet du contrôleur d'accès énuméré dans la décision de désignation, permettant aux utilisateurs finaux de sélectionner un autre service par défaut lorsque le système d'exploitation du contrôleur d'accès oriente les utilisateurs finaux vers ce moteur de recherche en ligne, cet assistant virtuel ou ce navigateur internet et lorsque l'assistant virtuel ou le navigateur internet du contrôleur d'accès oriente l'utilisateur vers le moteur de recherche en ligne énuméré dans la décision de désignation.

(50)

Les règles fixées par un contrôleur d'accès pour la distribution d'applications logicielles peuvent, dans certaines circonstances, restreindre la capacité des utilisateurs finaux d'installer et d'utiliser effectivement les applications logicielles ou les boutiques d'applications logicielles de tiers sur le matériel informatique ou les systèmes d'exploitation de ce contrôleur

d’accès, et restreindre également la capacité des utilisateurs finaux d’accéder à de telles applications logicielles ou boutiques d’applications logicielles sans passer par les services de plateforme essentiels de ce contrôleur d’accès. De telles restrictions peuvent limiter la capacité des développeurs d’applications logicielles d’utiliser d’autres canaux de distribution et la capacité des utilisateurs finaux de choisir entre les différentes applications logicielles de différents canaux de distribution, et devraient être interdites comme étant déloyales et susceptibles d’affaiblir la contestabilité des services de plateforme essentiels. Afin de garantir la contestabilité, le contrôleur d’accès devrait en outre permettre aux applications logicielles ou boutiques d’applications logicielles de tiers de demander à l’utilisateur final de décider si ce service devrait devenir le service par défaut et de permettre que le changement soit effectué facilement.

Le contrôleur d’accès concerné devrait pouvoir mettre en œuvre des mesures techniques ou contractuelles 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, s’il démontre que ces mesures sont nécessaires et justifiées et qu’il n’existe aucun moyen moins restrictif de préserver cette intégrité. L’intégrité du matériel informatique ou du système d’exploitation devrait inclure tous les choix de conception qui doivent être mis en œuvre et faire l’objet d’une maintenance pour protéger le matériel informatique ou le système d’exploitation contre tout accès non autorisé, en veillant à ce que les contrôles de sécurité spécifiés pour le matériel informatique ou le système d’exploitation concerné ne puissent être compromis. En outre, afin de garantir que les applications logicielles ou boutiques d’applications logicielles de tiers ne compromettent pas la sécurité des utilisateurs finaux, le contrôleur d’accès devrait pouvoir mettre en œuvre des mesures et des paramètres strictement nécessaires et proportionnés, autres que les paramètres par défaut, permettant aux utilisateurs finaux de garantir efficacement la sécurité, pour ce qui concerne les applications logicielles ou boutiques d’applications logicielles de tiers, si le contrôleur d’accès démontre que de telles mesures et de tels paramètres sont strictement nécessaires et justifiés et qu’il n’existe pas de moyens moins restrictifs d’atteindre cet objectif. Le contrôleur d’accès devrait être empêché de mettre en œuvre de telles mesures en tant que paramètres par défaut ou fonctionnalités préinstallées.

(51)

Les contrôleurs d’accès sont souvent verticalement intégrés et proposent certains produits ou services aux utilisateurs finaux par l’intermédiaire de leurs propres services de plateforme essentiels ou d’une entreprise utilisatrice sur laquelle ils exercent un contrôle, ce qui entraîne fréquemment des conflits d’intérêts. Cette situation se présente notamment lorsqu’un contrôleur d’accès fournit ses propres services d’intermédiation en ligne au travers d’un moteur de recherche en ligne. Lorsqu’ils proposent ces produits ou services dans le service de plateforme essentiel, les contrôleurs d’accès peuvent assurer une meilleure position, en termes de classement, ainsi que pour l’indexation et l’exploration qui y sont liées, à leur propre offre par rapport à celle des produits ou services des tiers également actifs dans ce service de plateforme essentiel. Cela peut notamment se produire avec des produits ou des services, y compris d’autres services de plateforme essentiels, qui sont classés parmi les résultats communiqués par des moteurs de recherche en ligne ou qui sont partiellement ou entièrement intégrés dans les résultats de moteurs de recherche en ligne, les groupes de résultats spécialisés dans un domaine défini, ou affichés avec les résultats d’un moteur de recherche en ligne, qui sont considérés ou utilisés par certains utilisateurs finaux comme un service distinct du moteur de recherche en ligne ou additionnel.

Les applications logicielles distribuées par l'intermédiaire de boutiques d'applications logicielles, ou les vidéos distribuées par l'intermédiaire de plateformes de partage de vidéos, ou les produits ou services mis en avant et affichés dans le fil d'actualité d'un service de réseau social en ligne, ou les produits ou services classés parmi des résultats de recherche ou affichés sur une place de marché en ligne, ou encore des produits ou services offerts par l'intermédiaire d'un assistant virtuel constituent d'autres exemples. Cette phase dans laquelle une position privilégiée est réservée à l'offre du contrôleur d'accès lui-même peut avoir lieu avant même qu'intervienne le classement à la suite d'une recherche, par exemple lors de l'exploration et de l'indexation. Par exemple, dès l'étape de l'exploration, un processus de découverte permettant de trouver des contenus nouveaux et mis à jour, ainsi que celle de l'indexation, qui implique le stockage et l'organisation des contenus trouvés au cours du processus d'exploration, le contrôleur d'accès peut favoriser son propre contenu par rapport à celui de tiers. Dans ces circonstances, le contrôleur d'accès joue un double rôle, en tant qu'intermédiaire vis-à-vis des entreprises tierces et en tant qu'entreprise fournissant directement des produits ou services. En conséquence, de tels contrôleurs d'accès sont en mesure de compromettre directement la contestabilité de ces produits ou services dans ces services de plateforme essentiels, au détriment des entreprises utilisatrices qui ne sont pas sous leur contrôle.

(52)

Dans ces circonstances, le contrôleur d'accès ne devrait accorder aux produits ou aux services qu'il fournit soit lui-même soit à travers une entreprise utilisatrice qu'il contrôle aucune forme de traitement différencié ou préférentiel en matière de classement, ainsi que pour l'indexation et l'exploration qui y sont liées, dans le service de plateforme essentiel, que ce soit par des moyens juridiques, commerciaux ou techniques. Afin que cette obligation soit effective, les conditions s'appliquant à un tel classement devraient être généralement équitables et transparentes. Dans ce contexte, le classement devrait couvrir toutes les formes de priorité relative, dont l'affichage, la notation, la création de liens hypertextes ou les résultats vocaux, et devrait également inclure les cas où un service de plateforme essentiel ne présente ou ne communique qu'un seul résultat à l'utilisateur final. Afin que cette obligation soit effective et ne puisse pas être contournée, il convient de l'appliquer également à toute mesure qui a un effet équivalent à un traitement différencié ou préférentiel en matière de classement. Les lignes directrices adoptées en vertu de l'article 5 du règlement (UE) 2019/1150 devraient également faciliter la mise en œuvre et le contrôle du respect de cette obligation.

(53)

Les contrôleurs d'accès ne devraient pas restreindre ou entraver le libre choix des utilisateurs finaux en empêchant techniquement ou de toute autre manière le changement vers d'autres applications logicielles ou services ou l'abonnement à d'autres applications logicielles ou services. Cela permettrait à un plus grand nombre d'entreprises de proposer leurs services, ce qui, en définitive, élargirait le choix offert aux utilisateurs finaux. Les contrôleurs d'accès devraient garantir ce libre choix, qu'ils soient ou non les fabricants du matériel informatique au moyen duquel se fait l'accès aux applications logicielles ou aux services, et ne devraient créer aucun obstacle artificiel, technique ou autre, visant à rendre impossible ou ineffectif le changement de plateforme. Ne devraient pas être considérées comme un obstacle interdit au changement de plateforme la simple offre d'un produit ou service donné aux consommateurs,

y compris au moyen d'une préinstallation, de même que l'amélioration de l'offre pour les utilisateurs finaux, telle que des prix plus avantageux ou une qualité supérieure.

(54)

Les contrôleurs d'accès peuvent entraver la capacité des utilisateurs finaux d'accéder aux contenus et services en ligne, y compris les applications logicielles. Par conséquent, il convient d'établir des règles visant à empêcher que le comportement des contrôleurs d'accès compromette les droits des utilisateurs finaux à accéder à un internet ouvert. De même, il se peut que les contrôleurs d'accès limitent techniquement la capacité des utilisateurs finaux de changer effectivement d'entreprise fournissant un service d'accès à l'internet, en particulier grâce au contrôle qu'ils exercent sur le matériel informatique ou les systèmes d'exploitation. Cela fausse les conditions de concurrence pour les services d'accès à l'internet et, en fin de compte, nuit aux utilisateurs finaux. Il convient donc de veiller à ce que les contrôleurs d'accès ne restreignent pas indûment le choix des utilisateurs finaux en ce qui concerne l'entreprise fournissant des services d'accès à l'internet.

(55)

Un contrôleur d'accès peut fournir des services ou du matériel informatique, comme des appareils portables, qui ont accès à des caractéristiques matérielles ou logicielles d'un appareil accessibles ou contrôlées par l'intermédiaire d'un système d'exploitation ou d'un assistant virtuel afin d'offrir des fonctionnalités spécifiques aux utilisateurs finaux. En pareil cas, les fournisseurs concurrents de services ou de matériel informatique, tels que les fournisseurs d'appareils portables, ont besoin d'une interopérabilité tout aussi effective avec les mêmes caractéristiques matérielles ou logicielles, ainsi que d'un accès à ces caractéristiques aux fins de l'interopérabilité, pour pouvoir proposer une offre concurrentielle aux utilisateurs finaux.

(56)

Les contrôleurs d'accès peuvent également jouer un double rôle en tant que développeurs de systèmes d'exploitation et en tant que fabricants d'appareils, y compris des fonctionnalités techniques qu'un appareil peut avoir. Par exemple, un contrôleur d'accès qui est également le fabricant d'un appareil peut restreindre l'accès à certaines des fonctionnalités de ce dernier, telles que la technologie de communication en champ proche, les éléments sécurisés et les processeurs, les mécanismes d'authentification et le logiciel utilisé pour exploiter ces technologies, qui peuvent être nécessaires à la fourniture effective d'un service, fournis conjointement au service de plateforme essentiel ou à l'appui de celui-ci, par le contrôleur d'accès ainsi que par toute entreprise tierce fournissant potentiellement un tel service.

(57)

Si les doubles rôles sont exercés d'une manière qui empêche d'autres fournisseurs de services ou de matériel informatique d'avoir accès dans les mêmes conditions aux mêmes caractéristiques du système d'exploitation, du matériel informatique ou du logiciel que celles qui sont disponibles ou utilisées par le contrôleur d'accès dans le cadre de la fourniture de ses propres services ou matériel informatique complémentaires ou d'appui, la capacité d'innovation de ces autres fournisseurs et le choix des utilisateurs finaux pourraient s'en trouver grandement compromis. Les contrôleurs d'accès devraient donc être tenus d'assurer, gratuitement, une interopérabilité effective avec les mêmes caractéristiques du système

d’exploitation, du matériel informatique ou du logiciel que celles qui sont disponibles ou utilisées dans le cadre de la fourniture de ses propres services et matériel informatique complémentaires et d’appui, ainsi que l’accès, aux fins de l’interopérabilité, à ces caractéristiques. Un tel accès peut également être exigé par des applications logicielles liées aux services concernés fournis conjointement au service de plateforme essentiel ou à l’appui de celui-ci afin de développer et offrir effectivement des fonctionnalités interopérables avec celles proposées par les contrôleurs d’accès. Ces obligations ont pour objet de permettre à des tiers concurrents de s’interconnecter, au moyen d’interfaces ou de solutions similaires, aux caractéristiques concernées de manière aussi effective que pour les propres services ou matériel informatique du contrôleur d’accès.

(58)

Les conditions dans lesquelles les contrôleurs d’accès fournissent des services de publicité en ligne aux entreprises utilisatrices, dont les annonceurs et les éditeurs, manquent souvent de transparence et sont opaques. Cela conduit souvent à un manque d’informations pour les annonceurs et éditeurs quant à l’effet d’une annonce publicitaire donnée. Dans le but de renforcer l’équité, la transparence et la contestabilité des services de publicité en ligne énumérés dans la décision de désignation, de même que ceux qui sont pleinement intégrés à d’autres services de plateforme essentiels de la même entreprise, les contrôleurs d’accès devraient fournir aux annonceurs et aux éditeurs, ainsi qu’aux tiers autorisés par les annonceurs et les éditeurs, sur demande, un accès gratuit à leurs outils de mesure de performance et aux données, tant agrégées que non agrégées, nécessaires aux annonceurs, aux tiers autorisés tels que les agences de publicité agissant pour le compte d’une entreprise de placement de publicité et aux éditeurs pour effectuer leur propre vérification indépendante de la fourniture des services de publicité en ligne concernés.

(59)

Les contrôleurs d’accès bénéficient d’un accès à de grandes quantités de données qu’ils collectent lorsqu’ils fournissent des services de plateforme essentiels, ainsi que d’autres services numériques. Afin d’empêcher les contrôleurs d’accès de nuire à la contestabilité des services de plateforme essentiels, ou au potentiel d’innovation d’un secteur numérique dynamique, en limitant le changement de plateforme ou le multihébergement, il convient d’accorder aux utilisateurs finaux, ainsi qu’aux tiers autorisés par un utilisateur final, un accès effectif et immédiat aux données qu’ils ont fournies ou qui ont été générées par leur activité sur les services de plateforme essentiels concernés du contrôleur d’accès. Les données devraient être reçues dans un format permettant qu’elles soient immédiatement et effectivement consultées et utilisées par l’utilisateur final ou le tiers concerné autorisé par l’utilisateur final à qui elles sont transmises. Les contrôleurs d’accès devraient également veiller, au moyen de mesures techniques appropriées et de haute qualité, telles que des interfaces de programmation, à ce que les utilisateurs finaux ou les tiers autorisés par les utilisateurs finaux puissent librement transférer les données en continu et en temps réel. Cela devrait également s’appliquer à toutes les autres données, à différents niveaux d’agrégation, nécessaires pour permettre effectivement cette portabilité. Pour éviter toute ambiguïté, l’obligation faite au contrôleur d’accès d’assurer la portabilité effective des données en vertu du présent règlement complète le droit à la portabilité des données prévu par le règlement (UE) 2016/679. Faciliter le changement de plateforme ou le multihébergement devrait ensuite permettre d’élargir le choix offert aux utilisateurs finaux et encourage les contrôleurs d’accès et les entreprises utilisatrices à innover.

(60)

Les entreprises utilisatrices de services de plateforme essentiels fournis par des contrôleurs d'accès et les utilisateurs finaux de ces entreprises utilisatrices fournissent et génèrent de grandes quantités de données. Afin que les entreprises utilisatrices puissent avoir accès aux données pertinentes ainsi générées, le contrôleur d'accès devrait, à leur demande, permettre un accès effectif et gratuit à ces données. Les tiers sous contrat avec l'entreprise utilisatrice, qui agissent en tant que sous-traitants de ces données pour cette entreprise, devraient également bénéficier d'un tel accès. Cet accès devrait inclure l'accès aux données fournies ou générées par les mêmes entreprises utilisatrices et les mêmes utilisateurs finaux de ces entreprises dans le cadre d'autres services fournis par le même contrôleur d'accès, y compris les services fournis conjointement aux services de plateforme essentiels ou à l'appui de ceux-ci lorsque cela est inextricablement lié à la demande concernée. À cette fin, un contrôleur d'accès ne devrait pas recourir à des restrictions contractuelles ou autres dans le but d'empêcher les entreprises utilisatrices d'accéder aux données pertinentes, et devrait permettre à ces entreprises utilisatrices d'obtenir le consentement de leurs utilisateurs finaux pour l'accès à ces données et leur extraction, lorsque ce consentement est requis en vertu du règlement (UE) 2016/679 et de la directive 2002/58/CE. Les contrôleurs d'accès devraient en outre garantir l'accès continu et en temps réel à de telles données au moyen de mesures techniques appropriées, par exemple en mettant en place des interfaces de programmation de haute qualité ou des outils intégrés pour les entreprises utilisatrices de petit volume.

(61)

Les moteurs de recherche en ligne gagnent en valeur pour leurs entreprises utilisatrices et leurs utilisateurs finaux respectifs à mesure que le nombre total de ces utilisateurs augmente. Les entreprises fournissant des moteurs de recherche en ligne collectent et conservent des ensembles de données agrégées contenant des informations sur les recherches effectuées par les utilisateurs, et la manière dont ces derniers ont interagi avec les résultats qu'ils ont obtenus. Les entreprises fournissant des moteurs de recherche en ligne collectent ces données à partir de recherches effectuées sur leur propre moteur de recherche en ligne et, le cas échéant, de recherches effectuées sur les plateformes de leurs partenaires commerciaux en aval. L'accès des contrôleurs d'accès à ces données concernant les classements, les requêtes, les clics et les vues constitue une barrière importante à l'entrée et à l'expansion, ce qui nuit à la contestabilité des moteurs de recherche en ligne. Les contrôleurs d'accès devraient donc être tenus de fournir aux autres entreprises fournissant de tels services, à des conditions équitables, raisonnables et non discriminatoires, un accès à ces données concernant les classements, les requêtes, les clics et les vues en lien avec les recherches gratuites et payantes générées par les consommateurs des moteurs de recherche en ligne, de manière à ce que ces entreprises tierces puissent optimiser leurs services et contester les services de plateforme essentiels concernés. Les tiers sous contrat avec le fournisseur d'un moteur de recherche en ligne, qui agissent en tant que sous-traitants de ces données pour ce moteur de recherche en ligne, devraient également bénéficier d'un tel accès. Lorsqu'il fournit un accès à ses données de recherche, un contrôleur d'accès devrait garantir la protection des données à caractère personnel des utilisateurs finaux, notamment contre les risques de réidentification, par des moyens adéquats, par exemple l'anonymisation des données à caractère personnel, sans altérer considérablement la qualité ou l'utilité des données. Les données concernées sont anonymisées si les données à caractères personnel sont irréversiblement modifiées de façon à ce que les informations ne soient plus liées à une personne physique identifiée ou identifiable,

ou si les données à caractère personnel sont rendues anonymes de telle manière que la personne concernée n'est pas ou n'est plus identifiable.

(62)

En ce qui concerne les boutiques d'applications logicielles, moteurs de recherche en ligne et services de réseaux sociaux en ligne énumérés dans la décision de désignation, les contrôleurs d'accès devraient publier et appliquer des conditions générales d'accès équitables, raisonnables et non discriminatoires. Ces conditions générales devraient prévoir un mécanisme de règlement extrajudiciaire des litiges au niveau de l'Union qui soit facilement accessible, impartial, indépendant et gratuit pour l'entreprise utilisatrice, sans préjudice de ses propres coûts et des mesures proportionnées visant à empêcher une utilisation abusive du mécanisme de règlement des litiges par les entreprises utilisatrices. Ce mécanisme de règlement des litiges devrait être sans préjudice du droit des entreprises utilisatrices de demander réparation devant les autorités judiciaires conformément au droit de l'Union et au droit national. En particulier, les contrôleurs d'accès qui fournissent un accès aux boutiques d'applications logicielles sont des points d'accès majeurs pour les entreprises utilisatrices qui cherchent à atteindre leurs utilisateurs finaux. Compte tenu du déséquilibre du pouvoir de négociation entre ces contrôleurs d'accès et les entreprises utilisatrices de leurs boutiques d'applications logicielles, ces contrôleurs d'accès ne devraient pas être autorisés à imposer des conditions générales, y compris en matière de tarification, qui seraient déloyales ou conduiraient à une différenciation injustifiée.

Les conditions tarifaires ou les autres conditions générales d'accès devraient être considérées comme déloyales si elles conduisent à un déséquilibre entre les droits et les obligations des entreprises utilisatrices, si elles confèrent au contrôleur d'accès un avantage qui est disproportionné par rapport au service qu'il fournit aux entreprises utilisatrices, ou si elles entraînent un désavantage pour les entreprises utilisatrices dans la fourniture de services identiques ou similaires à ceux du contrôleur d'accès. Les critères suivants peuvent servir à évaluer l'équité des conditions générales d'accès: les prix facturés ou les conditions imposées pour des services identiques ou similaires par d'autres fournisseurs de boutiques d'applications logicielles; les prix facturés ou les conditions imposées par le fournisseur de la boutique d'applications logicielles pour des services différents, liés ou similaires, ou à différents types d'utilisateurs finaux; les prix facturés ou les conditions imposées par le fournisseur de la boutique d'applications logicielles pour le même service dans différentes régions géographiques; les prix facturés ou les conditions imposées par le fournisseur de la boutique d'applications logicielles pour le même service que celui que le contrôleur d'accès se fournit à lui-même. Cette obligation ne devrait pas établir un droit d'accès et devrait être sans préjudice de la capacité des fournisseurs de boutiques d'applications logicielles, de moteurs de recherche en ligne et de services de réseaux sociaux en ligne d'assumer la responsabilité requise dans la lutte contre les contenus illicites et non désirés, comme le prévoit le règlement relatif au marché intérieur des services numériques.

(63)

Les contrôleurs d'accès peuvent entraver la capacité des entreprises utilisatrices et des utilisateurs finaux de se désabonner d'un service de plateforme essentiel auquel ils s'étaient précédemment abonnés. Par conséquent, il convient d'établir des règles afin d'éviter une situation dans laquelle les contrôleurs d'accès portent atteinte au droit des entreprises utilisatrices et des utilisateurs finaux de choisir librement le service de plateforme essentiel

qu’ils utilisent. Afin de préserver la liberté de choix des entreprises utilisatrices et des utilisateurs finaux, un contrôleur d’accès ne devrait pas être autorisé à rendre inutilement difficile ou compliqué, pour les entreprises utilisatrices ou les utilisateurs finaux, le désabonnement d’un service de plateforme essentiel. Il convient de ne pas rendre la clôture d’un compte ou le désabonnement d’un service plus compliqués que l’ouverture de ce compte ou l’abonnement à ce service. Les contrôleurs d’accès ne devraient pas exiger de frais supplémentaires lorsqu’ils résilient les contrats conclus avec leurs utilisateurs finaux ou entreprises utilisatrices. Les contrôleurs d’accès devraient veiller à ce que les conditions de résiliation des contrats soient toujours proportionnées et à ce que les utilisateurs finaux puissent les faire jouer sans difficultés excessives, par exemple en ce qui concerne les motifs de la résiliation, le délai de préavis ou la forme de la résiliation. Cela est sans préjudice de la législation nationale applicable conformément au droit de l’Union établissant des droits et obligations concernant les conditions de résiliation de la fourniture de services de plateforme essentiels par les utilisateurs finaux.

(64)

Le manque d’interopérabilité permet aux contrôleurs d’accès qui fournissent des services de communications interpersonnelles non fondés sur la numérotation de bénéficier d’effets de réseau importants, ce qui contribue à affaiblir la contestabilité. En outre, indépendamment de la question de savoir si les utilisateurs finaux optent ou non pour un «multihébergement», les contrôleurs d’accès fournissent souvent des services de communications interpersonnelles non fondés sur la numérotation dans le cadre de leur écosystème de plateforme, et cela exacerbe encore les barrières à l’entrée pour les autres fournisseurs de tels services et augmente les coûts de changement de fournisseur pour les utilisateurs finaux. Sans préjudice de la directive (UE) 2018/1972 du Parlement européen et du Conseil (14) et, en particulier, des conditions et procédures prévues à son article 61, les contrôleurs d’accès devraient donc assurer, gratuitement et sur demande, l’interopérabilité avec certaines fonctionnalités de base de leurs services de communications interpersonnelles non fondés sur la numérotation qu’ils fournissent à leurs propres utilisateurs finaux, pour les tiers fournisseurs de tels services.

Les contrôleurs d’accès devraient assurer l’interopérabilité pour les tiers fournisseurs de services de communications interpersonnelles non fondés sur la numérotation qui proposent ou entendent proposer ces services aux utilisateurs finaux et entreprises utilisatrices dans l’Union. Afin de faciliter la mise en œuvre pratique de cette interopérabilité, le contrôleur d’accès concerné devrait être tenu de publier une offre de référence énonçant les détails techniques et les conditions générales d’interopérabilité avec ses services de communications interpersonnelles non fondés sur la numérotation. La Commission devrait avoir la possibilité, le cas échéant, de consulter l’Organe des régulateurs européens des communications électroniques, afin de déterminer si les détails techniques et les conditions générales publiés dans l’offre de référence et que le contrôleur d’accès entend mettre en œuvre ou a mis en œuvre permettent de se conformer avec cette obligation.

Dans tous les cas, le contrôleur d’accès et le fournisseur demandeur devraient veiller à ce que l’interopérabilité ne compromette pas un niveau élevé de sécurité et de protection des données, conformément aux obligations qui leur incombent en vertu du présent règlement et du droit applicable de l’Union, en particulier le règlement (UE) 2016/679 et la directive 2002/58/CE. L’obligation relative à l’interopérabilité devrait être sans préjudice des informations et des choix à mettre à la disposition des utilisateurs finaux des services de communications interpersonnelles non fondés sur la numérotation du contrôleur d’accès et du

fournisseur demandeur en vertu du présent règlement et d'autres dispositions du droit de l'Union, en particulier du règlement (UE) 2016/679.

(65)

Pour garantir que les obligations prévues par le présent règlement soient effectives, tout en veillant à ce qu'elles se limitent à ce qui est nécessaire pour assurer la contestabilité et contrer les effets néfastes des pratiques déloyales des contrôleurs d'accès, il est important de les définir et circonscrire clairement, de manière à permettre au contrôleur d'accès de s'y conformer en tous points, tout en respectant pleinement le droit applicable, et en particulier le règlement (UE) 2016/679 et la directive 2002/58/CE ainsi que la législation sur la protection des consommateurs, la cybersécurité, la sécurité des produits et les exigences en matière d'accessibilité, y compris la directive (UE) 2019/882 et la directive (UE) 2016/2102 du Parlement européen et du Conseil (15). Les contrôleurs d'accès devraient garantir le respect du présent règlement dès la conception. Dès lors, les mesures nécessaires devraient être intégrées autant que possible dans la conception technologique utilisée par les contrôleurs d'accès.

Il peut, dans certains cas, être approprié pour la Commission, après avoir dialogué avec le contrôleur d'accès concerné, et après avoir permis aux tiers de présenter des observations, de préciser davantage certaines des mesures que le contrôleur d'accès devrait adopter afin de se conformer effectivement aux obligations susceptibles d'être précisées davantage ou, en cas de contournement, à toutes les obligations. En particulier, il devrait être possible d'apporter de telles précisions complémentaires lorsque la mise en œuvre d'une obligation susceptible d'être précisée peut être affectée par des variations de services au sein d'une seule catégorie de services de plateforme essentiels. À cet effet, le contrôleur d'accès devrait pouvoir demander à la Commission d'engager un processus dans le cadre duquel elle peut préciser davantage certaines des mesures que le contrôleur d'accès devrait adopter afin de se conformer effectivement à ces obligations.

La Commission devrait disposer d'un pouvoir d'appréciation quant à la question de savoir s'il y a lieu d'apporter des précisions complémentaires, et à quel moment, dans le respect de l'égalité de traitement, de la proportionnalité et du principe de bonne administration. À cet égard, la Commission devrait fournir les principales raisons qui sous-tendent son évaluation, y compris toute priorité pour le contrôle du respect de la législation. Ce processus ne devrait pas être utilisé pour nuire à l'efficacité du présent règlement. En outre, il est sans préjudice du pouvoir de la Commission d'adopter une décision constatant le non-respect, par un contrôleur d'accès, d'une des obligations énoncées dans le présent règlement, y compris de la possibilité d'infliger des amendes ou des astreintes. La Commission devrait pouvoir rouvrir une procédure, y compris lorsque les mesures précisées se révèlent inefficaces. Une réouverture due à l'inefficacité des précisions adoptées par voie de décision devrait permettre à la Commission de modifier ces précisions de manière prospective. La Commission devrait également être en mesure de fixer un délai raisonnable dans lequel la procédure peut être rouverte si les mesures précisées s'avèrent inefficaces.

(66)

Également pour garantir la proportionnalité, un contrôleur d'accès devrait avoir la possibilité de demander la suspension, dans la mesure nécessaire, d'une obligation spécifique dans des circonstances exceptionnelles échappant à son contrôle, telles qu'un choc externe imprévu le

privant temporairement d’une part considérable de la demande des utilisateurs finaux pour le service de plateforme essentiel concerné, s’il démontre que le respect de cette obligation particulière peut menacer la viabilité économique de ses activités dans l’Union. La Commission devrait déterminer les circonstances exceptionnelles justifiant la suspension et réexaminer celle-ci régulièrement pour évaluer si les conditions de son octroi sont toujours viables.

(67)

Dans des circonstances exceptionnelles, uniquement justifiées par des raisons de santé ou de sécurité publiques définies par le droit de l’Union et interprétées par la Cour de justice, la Commission devrait être en mesure de décider qu’une obligation donnée ne s’applique pas à un service de plateforme essentiel spécifique. Si une atteinte est portée à ces intérêts publics, cela pourrait indiquer que la mise en œuvre d’une obligation spécifique est, dans un cas exceptionnel précis, trop coûteuse pour la société dans son ensemble, et donc disproportionnée. Lorsqu’il y a lieu, la Commission devrait être en mesure de faciliter le respect en évaluant si une suspension ou exemption limitée et dûment motivée est justifiée. Cela devrait garantir la proportionnalité des obligations énoncées dans le présent règlement sans compromettre les effets ex ante escomptés sur l’équité et la contestabilité. Lorsqu’une exemption est accordée, la Commission devrait revoir sa décision tous les ans.

(68)

Dans le délai imparti pour respecter leurs obligations au titre du présent règlement, les contrôleurs d’accès devraient informer la Commission, par des rapports obligatoires, des mesures qu’ils comptent mettre en œuvre ou ont mis en œuvre afin d’assurer le respect effectif de ces obligations, y compris les mesures concernant le respect du règlement (UE) 2016/679, dans la mesure où elles sont pertinentes pour le respect des obligations prévues par le présent règlement, et qui devraient permettre à la Commission de s’acquitter de ses missions en vertu du présent règlement. En outre, il convient de rendre publique une synthèse non confidentielle claire et compréhensible de ces informations, tout en tenant compte de l’intérêt légitime des contrôleurs d’accès à la protection de leurs secrets d’affaires et autres informations confidentielles. Cette publication non confidentielle devrait permettre aux tiers d’évaluer si les contrôleurs d’accès respectent les obligations énoncées dans le présent règlement. Ces rapports devraient être sans préjudice de toute mesure d’exécution prise par la Commission à quelque moment que ce soit après ces rapports. La Commission devrait publier en ligne un lien vers la synthèse non confidentielle du rapport, ainsi que toutes les autres informations publiques à communiquer en application des obligations d’information prévues par le présent règlement, afin de garantir l’accessibilité desdites informations sous une forme utilisable et exhaustive, en particulier pour les petites et moyennes entreprises (PME).

(69)

Les obligations des contrôleurs d’accès ne devraient être actualisées qu’à la suite d’une enquête rigoureuse portant sur la nature et l’incidence de pratiques spécifiques qui pourraient être à leur tour désignées, après une enquête approfondie, comme étant déloyales ou limitant la contestabilité de la même manière que les pratiques déloyales décrites dans le présent règlement, tout en étant potentiellement exclues du champ d’application de l’ensemble actuel d’obligations. La Commission devrait pouvoir, soit de sa propre initiative, soit à la suite d’une demande motivée d’au moins trois États membres, ouvrir une enquête en vue de déterminer si

les obligations existantes doivent être actualisées. Lorsqu'ils présentent ces demandes motivées, les États membres devraient avoir la possibilité d'inclure des informations sur les offres nouvelles de produits, de services, de logiciels ou de caractéristiques qui suscitent des préoccupations du point de vue de la contestabilité ou de l'équité, qu'elles soient mises en œuvre dans le cadre de services de plateforme essentiels existants ou non. Lorsque, à la suite d'une enquête de marché, la Commission juge nécessaire de modifier des éléments essentiels du présent règlement, par exemple en incluant de nouvelles obligations qui s'écartent des mêmes questions de contestabilité ou d'équité que celles régies par le présent règlement, la Commission devrait présenter une proposition de modification du présent règlement.

(70)

Compte tenu du pouvoir économique considérable des contrôleurs d'accès, il est important que les obligations soient appliquées de manière effective et qu'elles ne soient pas contournées. À cette fin, les règles en question devraient s'appliquer à toute pratique d'un contrôleur d'accès, quelle que soit sa forme et indépendamment de sa nature contractuelle, commerciale, technique ou autre, dans la mesure où cette pratique correspond au type de pratique visé par l'une des obligations prévues par le présent règlement. Les contrôleurs d'accès ne devraient pas adopter un comportement susceptible de compromettre le caractère effectif des interdictions et obligations prévues par le présent règlement. Un tel comportement peut être la conception utilisée par le contrôleur d'accès, la présentation des choix de l'utilisateur final d'une façon qui n'est pas neutre ou l'utilisation de la structure, du fonctionnement ou du mode opératoire d'une interface utilisateur ou d'une partie de celle-ci pour réduire ou compromettre l'autonomie, la capacité décisionnelle ou le choix de l'utilisateur. En outre, le contrôleur d'accès ne devrait pas être autorisé à adopter un comportement compromettant l'interopérabilité exigée par le présent règlement, par exemple en recourant à des mesures techniques de protection injustifiées, à des conditions de service discriminatoires, en revendiquant illégalement un droit d'auteur sur des interfaces de programmation ou en fournissant des informations dénaturées. Les contrôleurs d'accès ne devraient pas être autorisés à contourner leur désignation en segmentant, divisant, subdivisant, fragmentant ou fractionnant artificiellement leurs services de plateforme essentiels dans le but de contourner les seuils quantitatifs fixés par le présent règlement.

(71)

Afin de garantir l'efficacité du réexamen du statut de contrôleur d'accès ainsi que la possibilité d'adapter la liste des services de plateforme essentiels fournis par un contrôleur d'accès, il convient que les contrôleurs d'accès informent la Commission de toutes les acquisitions prévues, avant leur mise en œuvre, d'autres entreprises fournissant des services de plateforme essentiels ou tout autre service dans le secteur numérique ou d'autres services qui permettent la collecte de données. De telles informations devraient non seulement servir au processus de réexamen en ce qui concerne le statut des contrôleurs d'accès individuels, mais aussi fournir des renseignements cruciaux pour le suivi des tendances plus générales en matière de contestabilité dans le secteur numérique; elles peuvent par conséquent être utilement prises en considération lors des enquêtes de marché prévues par le présent règlement. En outre, la Commission devrait communiquer ces informations aux États membres, étant donné qu'elles peuvent être utilisées à des fins de contrôle des concentrations au niveau national et que, dans certaines circonstances, l'autorité nationale compétente a la possibilité de soumettre ces acquisitions à la Commission aux fins du contrôle des concentrations. La Commission devrait également publier chaque année une liste des

acquisitions signalées par le contrôleur d'accès. Afin de garantir la nécessaire transparence de ces informations ainsi que leur utilité pour les différentes fins prévues par le présent règlement, les contrôleurs d'accès devraient fournir au moins les renseignements relatifs aux entreprises concernées par la concentration, leur chiffre d'affaires annuel dans l'Union et au niveau mondial, leur domaine d'activité, y compris les activités directement liées à la concentration, la valeur transactionnelle ou une estimation de celle-ci, un résumé relatif à la concentration, y compris sa nature et sa justification, ainsi qu'une liste des États membres concernés par l'opération.

(72)

Les intérêts des utilisateurs finaux en matière de protection des données et de la vie privée sont à prendre en considération pour toute appréciation des effets néfastes potentiels des pratiques des contrôleurs d'accès observées en ce qui concerne la collecte et l'accumulation de grandes quantités de données auprès des utilisateurs finaux. Assurer un niveau adéquat de transparence en ce qui concerne les pratiques de profilage utilisées par les contrôleurs d'accès, notamment mais pas uniquement le profilage au sens de l'article 4, point 4), du règlement (UE) 2016/679, permet de faciliter la contestabilité des services de plateforme essentiels. La transparence exerce une pression extérieure sur les contrôleurs d'accès pour ne pas faire du profilage approfondi du consommateur la norme dans le secteur, étant donné que les entrants potentiels ou les jeunes entreprises ne peuvent pas accéder à des données aussi étendues et profondes, et à une échelle similaire. Une plus grande transparence devrait permettre aux autres entreprises fournissant des services de plateforme essentiels de se démarquer davantage grâce à l'utilisation de garanties de protection de la vie privée plus performantes.

Afin d'assurer une efficacité minimale à cette obligation de transparence, les contrôleurs d'accès devraient fournir, au moins, une description, faisant l'objet d'un audit indépendant, de la base sur laquelle le profilage est effectué, en précisant si les données à caractère personnel et les données issues de l'activité de l'utilisateur, au sens du règlement (UE) 2016/679, sont utilisées, le traitement appliqué, les finalités pour lesquelles le profil est conçu et finalement utilisé, la durée du profilage, son incidence sur les services du contrôleur d'accès et les mesures prises pour permettre effectivement aux utilisateurs finaux d'avoir connaissance de l'utilisation voulue de ce profilage, de même que les mesures prises pour obtenir leur consentement ou leur donner la possibilité de le refuser ou de le retirer. La Commission devrait transférer la description faisant l'objet d'un audit au comité européen de la protection des données afin d'éclairer l'application des règles de l'Union en matière de protection des données. La Commission devrait être habilitée à mettre au point la méthodologie et la procédure pour la description devant faire l'objet d'un audit, en concertation avec le Contrôleur européen de la protection des données, le comité européen de la protection des données, la société civile et des experts, conformément aux règlements (UE) no 182/2011 (16) et (UE) 2018/1725 (17) du Parlement européen et du Conseil.

(73)

Afin de garantir la réalisation pleine et durable des objectifs du présent règlement, la Commission devrait être en mesure d'apprécier si une entreprise fournissant des services de plateforme essentiels doit être désignée comme contrôleur d'accès sans qu'elle atteigne les seuils quantitatifs fixés dans le présent règlement; si le non-respect systématique par un contrôleur d'accès justifie l'imposition de mesures correctives supplémentaires; s'il convient d'ajouter davantage de services relevant du secteur numérique à la liste des services de

plateforme essentiels; et si d'autres pratiques tout aussi déloyales et limitant également la contestabilité des marchés numériques doivent faire l'objet d'enquêtes. Cette appréciation devrait reposer sur des enquêtes de marché à conduire en temps opportun, moyennant des procédures et des délais clairs, afin de renforcer les effets ex ante du présent règlement sur la contestabilité et l'équité dans le secteur numérique, et de fournir le degré requis de sécurité juridique.

(74)

La Commission devrait être en mesure de constater, à la suite d'une enquête de marché, qu'une entreprise fournissant un service de plateforme essentiel remplit tous les critères qualitatifs globaux pour être désignée comme contrôleur d'accès. De ce fait, cette entreprise devrait, en principe, se conformer à toutes les obligations pertinentes prévues par le présent règlement. Toutefois, pour les contrôleurs d'accès qui ont été désignés par la Commission parce qu'il est prévisible qu'ils jouiront d'une position solide et durable dans un avenir proche, la Commission ne devrait imposer que les obligations nécessaires et appropriées pour les empêcher d'acquérir une position solide et durable dans leurs activités. En ce qui concerne ces contrôleurs d'accès émergents, la Commission devrait tenir compte de la nature en principe temporaire de ce statut et il faudra donc décider, en temps voulu, si une telle entreprise fournissant des services de plateforme essentiels devrait être soumise à l'ensemble des obligations imposées aux contrôleurs d'accès parce qu'elle a acquis une position solide et durable, ou si les conditions de désignation ne sont finalement pas satisfaites et si, par conséquent, toutes les obligations précédemment imposées devraient être levées.

(75)

La Commission devrait examiner et apprécier si des mesures correctives comportementales ou, le cas échéant, structurelles sont justifiées afin de veiller à ce que le contrôleur d'accès ne puisse contrarier les objectifs du présent règlement par le non-respect systématique d'au moins une des obligations qui y sont définies. Tel est le cas si la Commission a émis à l'encontre d'un contrôleur d'accès, sur une période de huit ans, au moins trois décisions constatant un non-respect, qui peuvent concerner des services de plateforme essentiels différents et différentes obligations prévues par le présent règlement, et si le contrôleur d'accès a maintenu, étendu ou encore renforcé son impact au sein du marché intérieur, la dépendance économique de ses entreprises utilisatrices et utilisateurs finaux vis-à-vis de ses services de plateforme essentiels ou la solidité de sa position. Un contrôleur d'accès devrait être réputé avoir maintenu, étendu ou renforcé sa position lorsque, malgré les mesures d'exécution prises par la Commission, il conserve ou a encore consolidé ou accru son importance en tant que point d'accès permettant aux entreprises utilisatrices d'atteindre les utilisateurs finaux.

La Commission devrait dans ces cas de figure avoir le pouvoir d'imposer toute mesure corrective, qu'elle soit comportementale ou structurelle, dans le respect du principe de proportionnalité. Dans ce contexte, la Commission devrait avoir le pouvoir d'interdire au contrôleur d'accès, dans la mesure où cette mesure corrective est proportionnée et nécessaire pour préserver ou rétablir l'équité et la contestabilité affectées par le non-respect systématique, pendant une période limitée, de procéder à une concentration concernant ces services de plateforme essentiels, les autres services fournis dans le secteur numérique ou les services permettant la collecte de données concernées par le non-respect systématique. Afin de permettre la participation effective de tiers et de donner la possibilité de tester les mesures

correctives avant de les appliquer, la Commission devrait publier une synthèse non confidentielle détaillée de la situation et des mesures à prendre. La Commission devrait être en mesure de rouvrir une procédure, y compris lorsque les mesures précisées se révèlent inefficaces. Une réouverture due à l'inefficacité de mesures correctives adoptées par voie de décision devrait permettre à la Commission de modifier les mesures correctives de manière prospective. La Commission devrait également être en mesure de fixer un délai raisonnable dans lequel il devrait être possible de rouvrir la procédure si les mesures correctives se révèlent inefficaces.

(76)

Lorsque, au cours d'une enquête portant sur un non-respect systématique, un contrôleur d'accès propose à la Commission de prendre des engagements, cette dernière devrait être en mesure d'adopter une décision rendant ces engagements obligatoires pour le contrôleur d'accès concerné, si elle estime que ces engagements garantissent le respect effectif des obligations énoncées dans le présent règlement. Cette décision devrait également constater qu'il n'y a plus lieu pour la Commission d'agir en ce qui concerne le non-respect systématique faisant l'objet de l'enquête. Lorsqu'elle évalue si les engagements que le contrôleur d'accès propose de prendre sont suffisants pour assurer le respect effectif des obligations prévues par le présent règlement, la Commission devrait être autorisée à tenir compte des tests effectués par le contrôleur d'accès pour démontrer l'efficacité pratique des engagements proposés. La Commission devrait vérifier que la décision relative aux engagements est pleinement respectée et atteint ses objectifs, et elle devrait être habilitée à rouvrir la décision si elle estime que les engagements ne sont pas efficaces.

(77)

Les services du secteur numérique et les types de pratiques liées à ces services peuvent évoluer rapidement et de façon considérable. Afin de veiller à ce que le présent règlement reste à jour et constitue une réponse réglementaire efficace et globale aux problèmes que posent les contrôleurs d'accès, il est important de prévoir un réexamen régulier des listes des services de plateforme essentiels, ainsi que des obligations prévues par le présent règlement. Cela est particulièrement important pour garantir qu'une pratique qui est susceptible de limiter la contestabilité des services de plateforme essentiels ou qui est déloyale soit mise en évidence. Bien qu'il importe de procéder régulièrement à des réexamens, compte tenu de l'évolution dynamique du secteur numérique, tout réexamen devrait être effectué dans un délai raisonnable et adéquat afin de procurer une sécurité juridique en ce qui concerne les conditions réglementaires. Les enquêtes de marché devraient également permettre à la Commission de disposer d'une base factuelle solide lui permettant d'apprécier si elle doit proposer de modifier le présent règlement de manière à réexaminer, élargir, ou détailler davantage les listes des services de plateforme essentiels. Elles devraient en outre permettre à la Commission de disposer d'une base factuelle solide lui permettant d'apprécier si elle doit proposer une modification des obligations prévues par le présent règlement, ou si elle doit adopter un acte délégué pour mettre à jour ces obligations.

(78)

En ce qui concerne les procédés des contrôleurs d'accès qui ne relèvent pas des obligations énoncées dans le présent règlement, la Commission devrait avoir la possibilité d'ouvrir une enquête de marché sur de nouveaux services et de nouvelles pratiques afin de déterminer si les

obligations énoncées dans le présent règlement doivent être complétées par un acte délégué relevant du champ d'application de l'habilitation établie pour de tels actes délégués dans le présent règlement, ou en présentant une proposition visant à modifier le présent règlement. Cette disposition est sans préjudice de la possibilité pour la Commission, dans les cas appropriés, d'intenter une procédure au titre de l'article 101 ou 102 du traité sur le fonctionnement de l'Union européenne. Ces procédures devraient être conduites conformément au règlement (CE) no 1/2003 du Conseil (18). Dans les cas d'urgence justifiés par le fait qu'un préjudice grave et irréparable risque d'être causé à la concurrence, la Commission devrait envisager d'adopter des mesures provisoires conformément à l'article 8 du règlement (CE) no 1/2003.

(79)

Si les contrôleurs d'accès se livrent à une pratique déloyale ou qui limite la contestabilité des services de plateforme essentiels déjà désignés en application du présent règlement, mais que cette pratique n'est pas explicitement couverte par les obligations prévues par le présent règlement, la Commission devrait être en mesure de mettre à jour le présent règlement au moyen d'actes délégués. Ces mises à jour par voie d'actes délégués devraient être soumises à la même norme en matière d'enquête et devraient donc être précédées d'une enquête de marché. La Commission devrait également appliquer une norme prédéfinie pour identifier ce type de pratiques. Cette norme juridique devrait donc garantir que le type d'obligations qui pourraient être imposées à tout moment aux contrôleurs d'accès en vertu du présent règlement est suffisamment prévisible.

(80)

Afin d'assurer la mise en œuvre et le respect effectifs du présent règlement, la Commission devrait disposer de pouvoirs d'enquête et de coercition étendus pour lui permettre d'enquêter, de faire respecter et de contrôler les règles énoncées dans le présent règlement, tout en veillant au respect du droit fondamental d'être entendu et d'accéder au dossier dans le cadre des procédures d'exécution. La Commission devrait en outre disposer de ces pouvoirs d'enquête pour mener des enquêtes de marché, y compris aux fins de la mise à jour et du réexamen du présent règlement.

(81)

La Commission devrait disposer dans toute l'Union du pouvoir de demander les renseignements nécessaires aux fins du présent règlement. La Commission devrait, en particulier, avoir accès à tous les documents, données, bases de données, algorithmes et informations pertinents nécessaires à l'ouverture et à la conduite d'enquêtes ainsi qu'au contrôle du respect des obligations énoncées dans le présent règlement, quel que soit le détenteur de ces informations, et indépendamment de leur forme, format, support de stockage ou lieu de conservation.

(82)

La Commission devrait pouvoir demander directement aux entreprises ou associations d'entreprises de fournir toutes preuves, données et informations pertinentes. De plus, la Commission devrait être en mesure de demander tout renseignement pertinent aux autorités compétentes d'un État membre, ou à toute personne physique ou morale aux fins du présent

règlement. Lorsqu'elles se conforment à la décision de la Commission, les entreprises sont tenues de répondre à des questions portant sur les faits et de fournir des documents.

(83)

La Commission devrait également être habilitée à procéder à l'inspection de toute entreprise ou association d'entreprises, à auditionner toute personne susceptible de disposer d'informations utiles et à enregistrer ses déclarations.

(84)

Les mesures provisoires peuvent constituer un instrument important pour garantir que l'infraction faisant l'objet d'une enquête en cours n'entraîne pas de préjudice grave et irréparable aux entreprises utilisatrices ou aux utilisateurs finaux des contrôleurs d'accès. Cet instrument joue un rôle important pour éviter une évolution qu'il serait très difficile d'inverser par une décision prise par la Commission à la fin de la procédure. La Commission devrait par conséquent avoir le pouvoir d'ordonner des mesures provisoires dans le cadre d'une procédure engagée en vue de l'adoption éventuelle d'une décision constatant un non-respect. Ce pouvoir devrait s'appliquer dans les cas où la Commission a constaté à première vue l'existence d'une infraction aux obligations qui incombent aux contrôleurs d'accès et où il existe un risque de préjudice grave et irréparable pour les entreprises utilisatrices ou les utilisateurs finaux des contrôleurs d'accès. Des mesures provisoires ne devraient s'appliquer que pour une durée déterminée, soit jusqu'au terme de la procédure engagée par la Commission, soit pour une période déterminée, qui peut être renouvelée dans la mesure où cela est nécessaire et opportun.

(85)

La Commission devrait pouvoir prendre les mesures nécessaires pour contrôler la mise en œuvre et le respect effectifs des obligations prévues par le présent règlement. Au titre de ces mesures, la Commission devrait avoir la capacité de nommer des experts externes indépendants et des auditeurs chargés de l'assister dans ce processus, y compris, le cas échéant, issus des autorités compétentes des États membres, par exemple les autorités chargées de la protection des données ou des consommateurs. Lors de la désignation des auditeurs, la Commission devrait assurer une rotation suffisante.

(86)

Le respect des obligations imposées par le présent règlement devrait pouvoir être assuré au moyen d'amendes et d'astreintes. À cette fin, il y a lieu de prévoir également des amendes et des astreintes d'un montant approprié en cas de non-respect des obligations et de violation des règles de procédure, sous réserve des délais de prescription appropriés, conformément aux principes de proportionnalité et ne bis in idem. La Commission et les autorités nationales compétentes devraient coordonner leurs efforts en matière de contrôle de l'application afin de veiller au respect des principes susmentionnés. En particulier, la Commission devrait tenir compte de toutes les amendes et astreintes imposées à la même personne morale pour les mêmes faits par une décision finale dans le cadre d'une procédure relative à une infraction à d'autres règles de l'Union ou nationales, de manière à veiller à ce que l'ensemble des amendes et astreintes imposées correspondent à la gravité des infractions commises.

(87)

Afin de garantir le recouvrement effectif d'une amende infligée à une association d'entreprises pour une infraction qu'elle a commise, il est nécessaire de fixer les conditions auxquelles il est possible pour la Commission d'exiger le paiement de l'amende auprès des entreprises membres de cette association d'entreprises lorsque celle-ci n'est pas solvable.

(88)

Dans le contexte des procédures menées au titre du présent règlement, il convient de consacrer le droit de l'entreprise intéressée d'être entendue par la Commission, et les décisions prises devraient faire l'objet d'une large publicité. Tout en assurant le droit à une bonne administration, le droit d'accès au dossier et le droit d'être entendu, il est indispensable de protéger les informations confidentielles. De plus, tout en respectant la confidentialité des informations, la Commission devrait garantir que toute information sur laquelle la décision repose est divulguée dans la mesure nécessaire pour que le destinataire de la décision comprenne les faits et les considérations qui ont guidé celle-ci. Il convient en outre de veiller à ce que la Commission n'utilise que des informations recueillies en vertu du présent règlement aux fins du présent règlement, sauf disposition expresse contraire. Enfin, il devrait être possible, dans certaines conditions, de considérer certains documents d'affaires, tels que les communications entre les avocats et leurs clients, comme confidentiels si les conditions applicables sont réunies.

(89)

Lorsqu'elle élabore des synthèses non confidentielles à publier afin de permettre effectivement aux tiers intéressés de présenter des observations, la Commission devrait tenir dûment compte de l'intérêt légitime des entreprises à la protection de leurs secrets d'affaires et autres informations confidentielles.

(90)

L'application cohérente, efficace et complémentaire des instruments juridiques disponibles aux contrôleurs d'accès nécessite une coopération et une coordination entre la Commission et les autorités nationales dans le cadre de leurs compétences. La Commission et les autorités nationales devraient coopérer et coordonner leurs actions nécessaires pour l'application des instruments juridiques disponibles aux contrôleurs d'accès au sens du présent règlement et respecter le principe de coopération loyale énoncé à l'article 4 du traité sur l'Union européenne. Le soutien qu'apportent les autorités nationales à la Commission devrait pouvoir comprendre la fourniture à cette dernière de toutes les informations nécessaires en leur possession ou, à la demande de celle-ci et dans l'exercice de ses compétences, d'une assistance qui lui permette de mieux pouvoir accomplir les tâches qui lui sont assignées par le présent règlement.

(91)

La Commission est la seule autorité habilitée à faire appliquer le présent règlement. Afin de soutenir la Commission, les États membres devraient avoir la possibilité d'habiliter leurs autorités nationales compétentes chargées de faire appliquer les règles de concurrence à mener des enquêtes sur d'éventuelles cas de non-respect par les contrôleurs d'accès de

certaines obligations prévues par le présent règlement. Cette démarche pourrait notamment se justifier lorsqu'il n'est pas possible de déterminer d'emblée si le comportement d'un contrôleur d'accès est de nature à constituer une infraction au présent règlement, aux règles de concurrence que l'autorité nationale compétente est habilitée à faire appliquer, ou aux deux. L'autorité nationale compétente chargée de faire appliquer les règles de concurrence devrait communiquer à la Commission un rapport sur ses constatations concernant d'éventuels cas de non-respect par les contrôleurs d'accès de certaines obligations prévues par le présent règlement, afin que celle-ci ouvre des procédures d'enquête sur tout cas de non-respect en tant que seule instance habilitée à faire appliquer les dispositions du présent règlement.

La Commission devrait avoir toute latitude pour décider d'ouvrir de telles procédures. Afin d'éviter un chevauchement des enquêtes menées au titre du présent règlement, l'autorité nationale compétente concernée devrait informer la Commission avant de prendre sa première mesure d'enquête sur un éventuel cas de non-respect par les contrôleurs d'accès de certaines obligations prévues par le présent règlement. Les autorités nationales compétentes devraient également agir en étroite coopération et coordination avec la Commission lorsqu'elles font appliquer les règles nationales de concurrence à l'encontre des contrôleurs d'accès, y compris en ce qui concerne la fixation d'amendes. À cette fin, elles devraient informer la Commission lorsqu'elles engagent une procédure fondée sur des règles nationales de concurrence à l'encontre des contrôleurs d'accès, ainsi qu'avant d'imposer des obligations aux contrôleurs d'accès dans le cadre d'une telle procédure. Afin d'éviter les doubles emplois, le fait d'informer du projet de décision conformément à l'article 11 du règlement (CE) no 1/2003 devrait pouvoir, le cas échéant, servir de notification au titre du présent règlement.

(92)

Afin de garantir que le présent règlement est appliqué et exécuté de façon harmonisée, il importe de veiller à ce que les autorités nationales, y compris les juridictions nationales, disposent de toutes les informations nécessaires pour s'assurer que leurs décisions ne soient pas contraires à une décision adoptée par la Commission en vertu du présent règlement. Les juridictions nationales devraient être autorisées à demander à la Commission de leur transmettre des informations ou des avis sur des questions concernant l'application du présent règlement. Dans le même temps, la Commission devrait pouvoir présenter des observations orales ou écrites aux juridictions nationales. Cette disposition est sans préjudice de la possibilité qu'ont les juridictions nationales d'introduire une demande de décision préjudicielle conformément à l'article 267 du traité sur le fonctionnement de l'Union européenne.

(93)

Afin d'assurer la cohérence et une complémentarité effective dans la mise en œuvre du présent règlement et d'autres réglementations sectorielles applicables aux contrôleurs d'accès, la Commission devrait bénéficier de l'expertise d'un groupe de haut niveau spécialisé. Ce groupe de haut niveau devrait également avoir la possibilité d'assister la Commission par le biais d'avis, d'expertise et de recommandations, le cas échéant, concernant des questions générales liées à la mise en œuvre ou à l'application du présent règlement. Le groupe de haut niveau devrait se composer des organes et réseaux européens concernés, et sa composition devrait garantir un niveau élevé d'expertise et un équilibre géographique. Les membres du groupe de haut niveau devraient régulièrement faire rapport aux organes et réseaux qu'ils représentent sur les tâches effectuées dans le cadre du groupe, et les consulter à cet égard.

(94)

Étant donné que les décisions prises par la Commission en application du présent règlement sont soumises au contrôle de la Cour de justice conformément au traité sur le fonctionnement de l'Union européenne, celle-ci devrait, conformément à l'article 261 du traité sur le fonctionnement de l'Union européenne, disposer d'une compétence de pleine juridiction en ce qui concerne les amendes et les astreintes.

(95)

La Commission devrait avoir la possibilité d'élaborer des lignes directrices pour fournir des orientations supplémentaires sur différents aspects du présent règlement ou pour aider les entreprises fournissant des services de plateforme essentiels à mettre en œuvre les obligations découlant du présent règlement. Ces orientations devraient pouvoir se fonder en particulier sur l'expérience acquise par la Commission dans le cadre du contrôle du respect du présent règlement. La publication de toute ligne directrice au titre du présent règlement est une prérogative et relève de la seule discrétion de la Commission et ne devrait pas être considérée comme un élément constitutif aux fins de veiller à ce que les entreprises ou associations d'entreprises concernées respectent les obligations qui leur incombent en vertu du présent règlement.

(96)

La mise en œuvre de certaines des obligations des contrôleurs d'accès, telles que celles liées à l'accès aux données, à leur portabilité ou à leur interopérabilité pourrait être facilitée par l'utilisation de normes techniques. À cet égard, la Commission devrait avoir la possibilité, lorsque cela est approprié et nécessaire, de demander aux organisations européennes de normalisation d'en élaborer.

(97)

Afin d'assurer la contestabilité et l'équité des marchés dans le secteur numérique de l'Union là où des contrôleurs d'accès opèrent, il convient de déléguer à la Commission le pouvoir d'adopter des actes conformément à l'article 290 du traité sur le fonctionnement de l'Union européenne afin de modifier la méthode qui figure dans une annexe du présent règlement et qui est utilisée pour déterminer si les seuils quantitatifs concernant les utilisateurs finaux actifs et les entreprises utilisatrices actives applicables à la désignation des contrôleurs d'accès sont atteints, afin de préciser davantage les éléments supplémentaires de la méthode qui ne figurent pas dans ladite annexe et qui permettent de déterminer si les seuils quantitatifs applicables à la désignation des contrôleurs d'accès sont atteints et afin de compléter les obligations existantes prévues dans le présent règlement, lorsque, sur la base d'une enquête de marché, la Commission a constaté qu'il fallait mettre à jour les obligations concernant les pratiques qui limitent la contestabilité des services de plateforme essentiels ou sont déloyales et que la mise à jour envisagée relève du champ d'application de l'habilitation établie pour de tels actes délégués dans le présent règlement.

(98)

Lorsqu'elle adopte des actes délégués en vertu du présent règlement, il importe particulièrement que la Commission procède aux consultations appropriées durant son travail préparatoire, y compris au niveau des experts, et que ces consultations soient menées conformément aux principes définis dans l'accord interinstitutionnel du 13 avril 2016«Mieux légiférer» (19). En particulier, pour assurer leur égale participation à la préparation des actes délégués, le Parlement européen et le Conseil reçoivent tous les documents au même moment que les experts des États membres, et leurs experts ont systématiquement accès aux réunions des groupes d'experts de la Commission traitant de la préparation des actes délégués.

(99)

Afin d'assurer des conditions uniformes d'exécution du présent règlement, il convient de conférer des compétences d'exécution à la Commission pour préciser les mesures à mettre en œuvre par les contrôleurs d'accès en vue de respecter effectivement les obligations leur incombant en vertu du présent règlement; pour suspendre, en tout ou en partie, une obligation spécifique imposée à un contrôleur d'accès; pour exempter un contrôleur d'accès, en tout ou en partie, d'une obligation spécifique; pour préciser les mesures à mettre en œuvre par un contrôleur d'accès lorsqu'il se soustrait aux obligations prévues par le présent règlement; pour mener à bien une enquête de marché en vue de la désignation des contrôleurs d'accès; pour imposer des mesures correctives en cas de non-respect systématique; pour ordonner des mesures provisoires à l'encontre d'un contrôleur d'accès; pour rendre des engagements obligatoires pour un contrôleur d'accès; pour établir son constat de non-respect; pour fixer le montant définitif de l'astreinte; pour déterminer la forme, la teneur et les autres modalités des notifications, des communications d'informations, des demandes motivées et des rapports réglementaires transmis par les contrôleurs d'accès; pour définir les modalités opérationnelles et techniques en vue de la mise en œuvre de l'interopérabilité ainsi que la méthodologie et la procédure pour la description, devant faire l'objet d'un audit, des techniques utilisées pour le profilage des consommateurs; pour prévoir les modalités pratiques des procédures, de la prolongation des délais, de l'exercice des droits au cours de la procédure, de la divulgation, ainsi que de la coopération et de la coordination entre la Commission et les autorités nationales. Ces compétences devraient être exercées conformément au règlement (UE) no 182/2011.

(100)

Il convient d'avoir recours à la procédure d'examen pour l'adoption d'un acte d'exécution relatif aux modalités pratiques de la coopération et de la coordination entre la Commission et les États membres. Il convient d'avoir recours à la procédure consultative pour les autres actes d'exécution prévus par le présent règlement. Cela se justifie par le fait que ces autres actes d'exécution ont trait à des aspects pratiques des procédures établies dans le présent règlement, tels que la forme, le contenu et d'autres détails des différentes étapes de la procédure, aux modalités pratiques des différentes étapes de la procédure, par exemple la prolongation des délais de procédure ou le droit d'être entendu, ainsi qu'aux décisions d'exécution individuelles adressées à un contrôleur d'accès.

(101)

Conformément au règlement (UE) no 182/2011, chaque État membre devrait être représenté au sein du comité consultatif et décider de la composition de sa délégation. Cette délégation

peut inclure, entre autres, des experts des autorités compétentes des États membres, qui possèdent l'expertise nécessaire pour une question spécifique présentée au comité consultatif.

(102)

Les lanceurs d'alerte peuvent porter à l'attention des autorités compétentes de nouvelles informations qui peuvent les aider à détecter les infractions au présent règlement et leur permettre d'imposer des sanctions. Il convient de veiller à ce que des dispositifs adéquats soient mis en place afin de permettre aux lanceurs d'alerte de prévenir les autorités compétentes en cas d'infraction potentielle ou avérée du présent règlement et de protéger ces lanceurs d'alerte contre des représailles. À cette fin, il convient de prévoir dans le présent règlement que la directive (UE) 2019/1937 du Parlement européen et du Conseil (20) s'applique au signalement de violations du présent règlement et à la protection des personnes signalant de telles violations.

(103)

En vue de renforcer la sécurité juridique, l'applicabilité, en vertu du présent règlement, de la directive (UE) 2019/1937 aux signalements de violations du présent règlement et à la protection des personnes qui signalent de telles violations devrait se refléter dans ladite directive. Il y a lieu de modifier en conséquence l'annexe de la directive (UE) 2019/1937. Il appartient aux États membres de veiller à ce que cette modification soit prise en compte dans leurs mesures de transposition adoptées conformément à la directive (UE) 2019/1937, bien que l'adoption de mesures de transposition nationales ne soit pas une condition de l'applicabilité de ladite directive, à compter de la date d'application du présent règlement, au signalement de violations du présent règlement et à la protection des personnes qui les signalent.

(104)

Les consommateurs devraient être autorisés à faire respecter leurs droits relatifs aux obligations imposées aux contrôleurs d'accès dans le cadre du présent règlement, au titre d'actions représentatives conformément à la directive (UE) 2020/1828 du Parlement européen et du Conseil (21). À cette fin, le présent règlement devrait prévoir que la directive (UE) 2020/1828 est applicable aux actions représentatives intentées en raison des infractions commises par des contrôleurs d'accès aux dispositions du présent règlement qui portent atteinte ou risquent de porter atteinte aux intérêts collectifs des consommateurs. Il y a donc lieu de modifier en conséquence l'annexe de ladite directive. Il appartient aux États membres de veiller à ce que cette modification soit prise en compte dans leurs mesures de transposition adoptées conformément à la directive (UE) 2020/1828, bien que l'adoption de mesures de transposition nationales à cet égard ne soit pas une condition de l'applicabilité de ladite directive à ces actions représentatives. L'applicabilité de la directive (UE) 2020/1828 aux actions représentatives intentées en raison des infractions commises par des contrôleurs d'accès aux dispositions du présent règlement qui portent atteinte ou risquent de porter atteinte aux intérêts collectifs des consommateurs devrait commencer à partir de la date d'application des dispositions législatives, réglementaires et administratives des États membres nécessaires à la transposition de ladite directive, ou à partir de la date d'application du présent règlement, la plus récente de ces dates étant retenue.

(105)

La Commission devrait évaluer périodiquement le présent règlement et suivre de près son incidence sur la contestabilité et l'équité des relations commerciales dans l'économie des plateformes en ligne, notamment en vue de déterminer la nécessité de modifications au regard des évolutions technologiques ou commerciales. Cette évaluation devrait comprendre le réexamen régulier de la liste des services de plateforme essentiels et des obligations imposées aux contrôleurs d'accès, ainsi que le contrôle de leur respect, dans le but d'assurer la contestabilité et l'équité des marchés numériques dans l'Union. Dans ce contexte, la Commission devrait également évaluer le champ de l'obligation concernant l'interopérabilité des services de communications électroniques non fondés sur la numérotation. Afin d'obtenir une vue d'ensemble de l'évolution du secteur numérique, l'évaluation devrait tenir compte des expériences des États membres et des parties prenantes concernées. À cet égard, la Commission devrait également avoir la possibilité de tenir compte des avis et rapports qui lui sont présentés par l'observatoire sur l'économie des plateformes en ligne instauré par la décision de la Commission C(2018) 2393 du 26 avril 2018. À la suite de l'évaluation, la Commission devrait prendre les mesures qui s'imposent. La Commission devrait avoir pour objectif le maintien d'un niveau élevé de protection et de respect des droits et valeurs communs, en particulier l'égalité et la non-discrimination, lorsqu'elle procède aux appréciations et réexamens des pratiques et des obligations énoncées dans le présent règlement.

(106)

Sans préjudice de la procédure budgétaire et grâce aux instruments financiers existants, il convient d'allouer à la Commission des ressources humaines, financières et techniques suffisantes pour lui permettre de s'acquitter efficacement de ses tâches et d'exercer les pouvoirs nécessaires à l'exécution du présent règlement.

(107)

Étant donné que l'objectif du présent règlement, à savoir assurer la contestabilité et l'équité du secteur numérique en général, et des services de plateforme essentiels en particulier, en vue d'encourager l'innovation, la qualité des produits et services numériques, l'équité et la compétitivité des prix, ainsi qu'un niveau élevé de qualité et de choix pour les utilisateurs finaux dans le secteur numérique, ne peut pas être atteint de manière suffisante par les États membres mais peut, en raison du modèle commercial et des activités des contrôleurs d'accès, ainsi que de l'ampleur et des effets de ces activités, l'être mieux au niveau de l'Union, celle-ci peut prendre des mesures, conformément au principe de subsidiarité consacré à l'article 5 du traité sur l'Union européenne. Conformément au principe de proportionnalité énoncé audit article, le présent règlement n'excède pas ce qui est nécessaire pour atteindre cet objectif.

(108)

Le Contrôleur européen de la protection des données a été consulté conformément à l'article 42 du règlement (UE) 2018/1725 et a rendu un avis le 10 février 2021 (22).

(109)

Le présent règlement respecte les droits fondamentaux et observe les principes reconnus par la Charte des droits fondamentaux de l'Union européenne, notamment ses articles 16, 47 et 50.

En conséquence, l’interprétation et l’application du présent règlement devraient observer ces droits et principes,

ONT ADOPTÉ LE PRÉSENT RÈGLEMENT:

CHAPITRE I

OBJET, CHAMP D’APPLICATION ET DÉFINITIONS

Article premier

Objet et champ d’application

1. L’objectif du présent règlement est de contribuer au bon fonctionnement du marché intérieur, en établissant des règles harmonisées visant à garantir à toutes les entreprises la contestabilité et l’équité des marchés dans le secteur numérique de l’Union là où des contrôleurs d’accès sont présents, au profit des entreprises utilisatrices et des utilisateurs finaux.

2. Le présent règlement s’applique aux services de plateforme essentiels fournis ou proposés par des contrôleurs d’accès à des entreprises utilisatrices établies dans l’Union ou à des utilisateurs finaux établis ou situés dans l’Union, quel que soit le lieu d’établissement ou de résidence des contrôleurs d’accès et quel que soit le droit par ailleurs applicable à la fourniture des services.

3. Le présent règlement ne s’applique pas aux marchés liés:

a)

aux réseaux de communications électroniques au sens de l’article 2, point 1), de la directive (UE) 2018/1972;

b)

aux services de communications électroniques au sens de l’article 2, point 4), de la directive (UE) 2018/1972, autres que ceux liés aux services de communications interpersonnelles non fondés sur la numérotation.

4. En ce qui concerne les services de communications interpersonnelles au sens de l’article 2, point 5), de la directive (UE) 2018/1972, le présent règlement est sans préjudice des pouvoirs et responsabilités confiés aux autorités de régulation nationales et autres autorités compétentes en vertu de l’article 61 de ladite directive.

5. Afin d’éviter la fragmentation du marché intérieur, les États membres n’imposent pas d’obligations supplémentaires aux contrôleurs d’accès par voie législative, réglementaire ou de mesures administratives aux fins de garantir la contestabilité et l’équité des marchés. Aucune disposition du présent règlement n’empêche les États membres d’imposer aux entreprises, y compris les entreprises fournissant des services de plateforme essentiels, des obligations sur des points ne relevant pas du champ d’application du présent règlement, pour autant que ces obligations soient compatibles avec le droit de l’Union et ne résultent pas du

fait que les entreprises concernées ont le statut d'un contrôleur d'accès au sens du présent règlement.

6. Le présent règlement est sans préjudice de l'application des articles 101 et 102 du traité sur le fonctionnement de l'Union européenne. Il est également sans préjudice de l'application:

a)

des règles de concurrence nationales interdisant les accords anticoncurrentiels, les décisions d'associations d'entreprises, les pratiques concertées et les abus de position dominante;

b)

des règles de concurrence nationales interdisant d'autres formes de comportement unilatéral, dans la mesure où elles s'appliquent à des entreprises autres que les contrôleurs d'accès ou reviennent à imposer des obligations supplémentaires aux contrôleurs d'accès; et

c)

du règlement (CE) no 139/2004 du Conseil (23) et des règles nationales relatives au contrôle des concentrations.

7. Les autorités nationales ne prennent aucune décision qui va à l'encontre d'une décision adoptée par la Commission en vertu du présent règlement. La Commission et les États membres travaillent en étroite coopération et coordonnent leurs mesures d'exécution en se fondant sur les principes établis aux articles 37 et 38.

Article 2

Définitions

Aux fins du présent règlement, on entend par:

1)

«contrôleur d'accès»: une entreprise fournissant des services de plateforme essentiels, désignée conformément à l'article 3;

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)

navigateurs internet;

h)

assistants virtuels;

i)

services d’informatique en nuage;

j)

services de publicité en ligne, y compris tout réseau publicitaire, échange publicitaire et autre service d’intermédiation publicitaire, fourni par une entreprise qui met à disposition n’importe lequel des services de plateforme essentiels énumérés aux points a) à i);

3)

«service de la société de l’information»: tout service au sens de l’article 1er, paragraphe 1, point b), de la directive (UE) 2015/1535;

4)

«secteur numérique»: le secteur des produits et services fournis au moyen ou par l’intermédiaire de services de la société de l’information;

5)

«services d’intermédiation en ligne»: les services d’intermédiation en ligne au sens de l’article 2, point 2), du règlement (UE) 2019/1150;

6)

«moteur de recherche en ligne»: un moteur de recherche en ligne au sens de l'article 2, point 5), du règlement (UE) 2019/1150;

7)

«service de réseaux sociaux en ligne»: une plateforme permettant aux utilisateurs finaux de se connecter ainsi que de communiquer entre eux, de partager des contenus et de découvrir d'autres utilisateurs et d'autres contenus, sur plusieurs appareils et, en particulier, au moyen de conversations en ligne (chats), de publications (posts), de vidéos et de recommandations;

8)

«service de plateformes de partage de vidéos»: un service de plateformes de partage de vidéos au sens de l'article 1er, paragraphe 1, point a bis), de la directive 2010/13/UE;

9)

«service de communications interpersonnelles non fondé sur la numérotation»: un service de communications interpersonnelles non fondé sur la numérotation au sens de l'article 2, point 7), de la directive (UE) 2018/1972;

10)

«système d'exploitation»: un logiciel système qui contrôle les fonctions de base du matériel informatique ou du logiciel et permet d'y faire fonctionner des applications logicielles;

11)

«navigateur internet»: une application logicielle qui permet aux utilisateurs finaux d'accéder à des contenus internet hébergés sur des serveurs connectés à des réseaux tels que l'internet, y compris les navigateurs internet autonomes, ainsi que les navigateurs internet intégrés ou inclus dans un logiciel ou équivalent, et d'interagir avec ces contenus;

12)

«assistant virtuel»: un logiciel qui peut traiter des demandes, des tâches ou des questions, notamment celles fondées sur des données d'entrée sonores, visuelles ou écrites, de gestes ou de mouvements, et qui, sur la base de ces demandes, tâches ou questions, donne accès à d'autres services ou contrôle des appareils connectés physiques;

13)

«service d'informatique en nuage»: un service d'informatique en nuage au sens de l'article 4, point 19), de la directive (UE) 2016/1148 du Parlement européen et du Conseil (24);

14)

«boutique d'applications logicielles»: un type de services d'intermédiation en ligne qui se concentre sur les applications logicielles en tant que produit ou service intermédié;

15)

«application logicielle»: tout produit ou service numérique fonctionnant sur un système d’exploitation;

16)

«service de paiement»: un service de paiement au sens de l’article 4, point 3), de la directive (UE) 2015/2366;

17)

«service technique à l’appui d’un service de paiement»: un service au sens de l’article 3, point j), de la directive (UE) 2015/2366;

18)

«système de paiement pour les achats intégrés à des applications»: une application logicielle, un service ou une interface utilisateur qui facilite les achats de contenu numérique ou de services numériques dans une application logicielle, y compris en termes de contenu, d’abonnements, de caractéristiques ou de fonctionnalité, ainsi que les paiements pour de tels achats;

19)

«service d’identification»: un type de service fourni avec ou à l’appui des services de plateforme essentiels permettant toute sorte de vérification de l’identité des utilisateurs finaux ou des entreprises utilisatrices, indépendamment de la technologie utilisée;

20)

«utilisateur final»: toute personne physique ou morale utilisant des services de plateforme essentiels autrement qu’en tant qu’entreprise utilisatrice;

21)

«entreprise utilisatrice»: toute personne physique ou morale agissant à titre commercial ou professionnel qui utilise des services de plateforme essentiels aux fins ou dans le cadre de la fourniture de biens ou de services à des utilisateurs finaux;

22)

«classement»: la priorité relative accordée aux biens ou services proposés par le biais de services d’intermédiation en ligne, de services de réseaux sociaux en ligne, de services de plateformes de partage de vidéos ou d’assistants virtuels, ou la pertinence reconnue aux résultats de recherche par les moteurs de recherche en ligne, tels qu’ils sont présentés, organisés ou communiqués par les entreprises fournissant des services d’intermédiation en ligne, des services de plateformes de partage de vidéos, des assistants virtuels ou des moteurs de recherche en ligne, indépendamment des moyens technologiques utilisés pour une telle

présentation, organisation ou communication et indépendamment du fait qu'un seul résultat soit ou non présenté ou communiqué;

23)

«résultats de recherche»: toute information, sous quelque format que ce soit, y compris des données textuelles, graphiques, vocales ou autres, renvoyées en réponse à une recherche, et en rapport avec celle-ci, que l'information renvoyée soit un résultat payant ou non, une réponse directe ou tout produit, service ou renseignement proposé en lien avec les résultats organiques, affiché en même temps que ceux-ci ou partiellement ou entièrement intégré dans ceux-ci;

24)

«données»: toute représentation numérique d'actes, de faits ou d'informations et toute compilation de ces actes, faits ou informations, notamment sous la forme d'enregistrements sonores, visuels ou audiovisuels;

25)

«données à caractère personnel»: les données à caractère personnel au sens de l'article 4, point 1), du règlement (UE) 2016/679;

26)

«données à caractère non personnel»: les données autres que les données à caractère personnel;

27)

«entreprise»: une entité exerçant une activité économique, indépendamment de son statut juridique et de son mode de financement, y compris toutes les entreprises liées ou connectées formant un groupe par l'intermédiaire du contrôle direct ou indirect d'une entreprise par une autre;

28)

«contrôle»: la possibilité d'exercer une influence déterminante sur l'activité d'une entreprise, au sens de l'article 3, paragraphe 2, du règlement (CE) no 139/2004;

29)

«interopérabilité»: la capacité d'échanger des informations et d'utiliser mutuellement les informations échangées par le biais d'interfaces ou d'autres solutions, de telle sorte que tous les éléments du matériel informatique ou des logiciels fonctionnent de toutes les manières dont elles sont censées fonctionner avec d'autres matériels informatiques et logiciels ainsi qu'avec les utilisateurs;

30)

«chiffre d’affaires»: le montant réalisé par une entreprise au sens de l’article 5, paragraphe 1, du règlement (CE) no 139/2004;

31)

«profilage»: le profilage au sens de l’article 4, point 4), du règlement (UE) 2016/679;

32)

«consentement»: le consentement au sens de l’article 4, point 11), du règlement (UE) 2016/679;

33)

«juridiction nationale»: toute juridiction d’un État membre au sens de l’article 267 du traité sur le fonctionnement de l’Union européenne.

CHAPITRE II

CONTRÔLEURS D’ACCÈS

Article 3

Désignation des contrôleurs d’accès

1. Une entreprise est désignée comme étant un contrôleur d’accès si:

a)

elle a un poids important sur le marché intérieur;

b)

elle fournit un service de plateforme essentiel qui constitue un point d’accès majeur permettant aux entreprises utilisatrices d’atteindre leurs utilisateurs finaux; et

c)

elle jouit d’une position solide et durable, dans ses activités, ou jouira, selon toute probabilité, d’une telle position dans un avenir proche.

2. Une entreprise est réputée satisfaire aux exigences respectives du paragraphe 1:

a)

en ce qui concerne le paragraphe 1, point a), si elle a réalisé un chiffre d’affaires annuel dans l’Union supérieur ou égal à 7,5 milliards d’euros au cours de chacun des trois derniers exercices, ou si sa capitalisation boursière moyenne ou sa juste valeur marchande équivalente a atteint au moins 75 milliards d’euros au cours du dernier exercice, et qu’elle fournit le même service de plateforme essentiel dans au moins trois États membres;

b)

en ce qui concerne le paragraphe 1, point b), si elle fournit un service de plateforme essentiel qui, au cours du dernier exercice, a compté au moins 45 millions d'utilisateurs finaux actifs par mois établis ou situés dans l'Union et au moins 10 000 entreprises utilisatrices actives par an établies dans l'Union, faisant l'objet d'une identification et de calculs conformément à la méthode et aux indicateurs définis dans l'annexe;

c)

en ce qui concerne le paragraphe 1, point c), si les seuils visés au point b) du présent paragraphe ont été atteints au cours de chacun des trois derniers exercices.

3. Lorsqu'une entreprise fournissant des services de plateforme essentiels atteint l'ensemble des seuils mentionnés au paragraphe 2, elle en informe la Commission sans tarder et, en tout état de cause, dans les deux mois qui suivent après que ces seuils ont été atteints et lui fournit les informations pertinentes visées au paragraphe 2. Cette notification inclut les informations pertinentes visées au paragraphe 2 pour chacun des services de plateforme essentiels de l'entreprise qui atteint les seuils mentionnés au paragraphe 2, point b). Lorsqu'un autre service de plateforme essentiel fourni par l'entreprise qui a précédemment été désignée comme étant un contrôleur d'accès atteint les seuils mentionnés au paragraphe 2, points b) et c), cette entreprise en informe la Commission dans les deux mois qui suivent le respect de ces seuils.

Lorsque l'entreprise fournissant le service de plateforme essentiel n'informe pas la Commission conformément au premier alinéa du présent paragraphe et qu'elle ne parvient pas à fournir, dans le délai fixé par la Commission dans la demande de renseignements visée à l'article 21, tous les renseignements pertinents dont la Commission a besoin pour désigner l'entreprise concernée en tant que contrôleur d'accès en vertu du paragraphe 4 du présent article, la Commission conserve le droit de désigner cette entreprise en tant que contrôleur d'accès, sur la base des informations dont elle dispose.

Lorsque l'entreprise fournissant des services de plateforme essentiels se conforme à la demande de renseignement en vertu du deuxième alinéa du présent paragraphe ou que les renseignements sont fournis après l'expiration du délai visé à cet alinéa, la Commission applique la procédure prévue au paragraphe 4.

4. La Commission désigne comme étant un contrôleur d'accès, sans retard indu et au plus tard dans un délai de 45 jours ouvrables après avoir reçu toutes les informations visées au paragraphe 3, une entreprise fournissant des services de plateforme essentiels qui atteint tous les seuils mentionnés au paragraphe 2.

5. L'entreprise fournissant des services de plateforme essentiels peut présenter, avec sa notification, des arguments suffisamment étayés pour démontrer que, exceptionnellement, bien qu'elle atteigne tous les seuils prévus au paragraphe 2 et en raison des circonstances dans lesquelles le service de plateforme essentiel concerné opère, elle ne satisfait pas aux exigences énumérées au paragraphe 1.

Lorsque la Commission estime que les arguments présentés en vertu du premier alinéa par l'entreprise fournissant des services de plateforme essentiels ne sont pas suffisamment étayés parce qu'ils ne remettent manifestement pas en cause les présomptions énoncées au paragraphe 2 du présent article, elle peut rejeter ces arguments dans le délai visé au paragraphe 4, sans appliquer la procédure prévue à l'article 17, paragraphe 3.

Lorsque l'entreprise fournissant des services de plateforme essentiels présente de tels arguments suffisamment étayés, remettant manifestement en cause les présomptions mentionnées au paragraphe 2 du présent article, la Commission peut, nonobstant le premier alinéa du présent paragraphe et dans le délai visé au paragraphe 4 du présent article, ouvrir la procédure prévue à l'article 17, paragraphe 3.

Si la Commission conclut que l'entreprise fournissant des services de plateforme essentiels n'a pas été en mesure de démontrer que les services de plateforme essentiels qu'elle fournit ne satisfont pas aux exigences du paragraphe 1 du présent article, elle désigne cette entreprise comme étant un contrôleur d'accès conformément à la procédure prévue à l'article 17, paragraphe 3.

6. La Commission est habilitée à adopter des actes délégués conformément à l'article 49 afin de compléter le présent règlement en précisant la méthode utilisée pour déterminer si les seuils quantitatifs fixés au paragraphe 2 du présent article sont atteints, et d'adapter régulièrement ladite méthode, le cas échéant, aux évolutions du marché et de la technologie.

7. La Commission est habilitée à adopter des actes délégués conformément à l'article 49 afin de modifier le présent règlement en mettant à jour la méthode et la liste des indicateurs définies dans l'annexe.

8. La Commission désigne comme étant un contrôleur d'accès, conformément à la procédure prévue à l'article 17, toute entreprise fournissant des services de plateforme essentiels qui satisfait à chacune des exigences visées au paragraphe 1 du présent article, mais n'atteint pas chacun des seuils mentionnés au paragraphe 2 du présent article.

À cette fin, la Commission tient compte de tout ou partie des éléments ci-après, pour autant qu'ils soient pertinents pour l'entreprise considérée fournissant des services de plateforme essentiels:

a)

la taille, y compris le chiffre d'affaires et la capitalisation boursière, les activités et la position de ladite entreprise;

b)

le nombre d'entreprises utilisatrices qui font appel au service de plateforme essentiel pour atteindre des utilisateurs finaux et le nombre d'utilisateurs finaux;

c)

les effets de réseau et les avantages tirés des données, en particulier en ce qui concerne l'accès aux données à caractère personnel et non personnel et la collecte de ces données par ladite entreprise, ou les capacités d'analyse de cette dernière;

d)

tout effet d'échelle et de gamme dont bénéficie l'entreprise, y compris en ce qui concerne les données et, le cas échéant, ses activités en dehors de l'Union;

e)

la captivité des entreprises utilisatrices ou des utilisateurs finaux, y compris les coûts de changement et les biais comportementaux qui réduisent la capacité des entreprises utilisatrices et des utilisateurs finaux à changer de fournisseur ou à opter pour un multihébergement;

f)

une structure d'entreprise conglomérale ou l'intégration verticale de cette entreprise, permettant par exemple à celle-ci de pratiquer des subventions croisées, de combiner des données provenant de différentes sources ou de tirer parti de sa position; ou

g)

d'autres caractéristiques structurelles des entreprises ou des services.

Dans le cadre de la réalisation de son appréciation au titre du présent paragraphe, la Commission tient compte de l'évolution prévisible en relation avec les éléments énumérés au deuxième alinéa, y compris tout projet de concentration faisant intervenir une autre entreprise fournissant des services de plateforme essentiels ou tout autre service dans le secteur numérique ou permettant la collecte de données.

Si une entreprise fournissant un service de plateforme essentiel qui n'atteint pas les seuils quantitatifs visés au paragraphe 2 ne se conforme pas de manière substantielle aux mesures d'enquête ordonnées par la Commission et si ce manquement persiste après que cette entreprise a été invitée à s'y conformer dans un délai raisonnable et à soumettre ses observations, la Commission peut désigner cette entreprise comme étant un contrôleur d'accès sur la base des faits dont dispose la Commission.

9. Pour chaque entreprise désignée comme étant un contrôleur d'accès en vertu du paragraphe 4 ou 8, la Commission énumère dans la décision de désignation les services de plateforme essentiels concernés qui sont fournis au sein de cette entreprise et qui constituent, individuellement, des points d'accès majeurs permettant aux entreprises utilisatrices d'atteindre les utilisateurs finaux, comme indiqué au paragraphe 1, point b).

10. Le contrôleur d'accès se conforme aux obligations prévues aux articles 5, 6 et 7 dans les six mois suivant l'énumération d'un service de plateforme essentiel dans la décision de désignation conformément au paragraphe 9 du présent article.

Article 4

Réexamen du statut de contrôleur d’accès

1. La Commission peut, sur demande ou de sa propre initiative, revoir, modifier ou abroger à tout moment une décision de désignation adoptée au titre de l’article 3 pour l’une des raisons suivantes:

a)

l’un des faits sur lesquels la décision de désignation repose subit un changement important;

b)

la décision de désignation repose sur des informations incomplètes, inexactes ou dénaturées.

2. La Commission réexamine régulièrement, et au moins tous les trois ans, si les contrôleurs d’accès continuent de satisfaire aux exigences fixées à l’article 3, paragraphe 1. Ce réexamen détermine également s’il faut modifier la liste des services de plateforme essentiels du contrôleur d’accès qui constituent, individuellement, des points d’accès majeurs permettant aux entreprises utilisatrices d’atteindre les utilisateurs finaux, comme indiqué à l’article 3, paragraphe 1, point b). Ces réexamens n’ont pas d’effet suspensif sur les obligations du contrôleur d’accès.

La Commission examine également au moins une fois par an si de nouvelles entreprises fournissant des services de plateforme essentiels satisfont à ces exigences.

Si la Commission constate, sur la base des examens menés conformément au premier alinéa, que les faits sur lesquels repose la désignation des entreprises fournissant des services de plateforme essentiels comme contrôleurs d’accès ont évolué, elle adopte une décision confirmant, modifiant ou abrogeant la décision de désignation.

3. La Commission publie et tient à jour de façon continue une liste des contrôleurs d’accès et la liste des services de plateforme essentiels pour lesquels ils doivent se conformer aux obligations prévues au chapitre III.

CHAPITRE III

PRATIQUES DES CONTRÔLEURS D’ACCÈS QUI LIMITENT LA CONTESTABILITÉ OU SONT DÉLOYALES

Article 5

Obligations incombant aux contrôleurs d’accès

1. Le contrôleur d’accès se conforme à toutes les obligations énoncées au présent article pour chacun de ses services de plateforme essentiels énumérés dans la décision de désignation conformément à l’article 3, paragraphe 9.

2. Tout contrôleur d’accès est tenu de ne pas:

a)

traiter, aux fins de la fourniture de services de publicité en ligne, les données à caractère personnel des utilisateurs finaux qui recourent à des services de tiers utilisant des services de plateforme essentiels fournis par le contrôleur d'accès;

b)

combiner les données à caractère personnel provenant du service de plateforme essentiel concerné avec les données à caractère personnel provenant de tout autre service de plateforme essentiel ou de tout autre service fourni par le contrôleur d'accès, ni avec des données à caractère personnel provenant de services tiers;

c)

utiliser de manière croisée les données à caractère personnel provenant du service de plateforme essentiel concerné dans le cadre d'autres services fournis séparément par le contrôleur d'accès, y compris d'autres services de plateforme essentiels, et inversement; et

d)

inscrire les utilisateurs finaux à d'autres services du contrôleur d'accès dans le but de combiner des données à caractère personnel,

à moins que ce choix précis ait été présenté à l'utilisateur final et que ce dernier ait donné son consentement au sens de l'article 4, point 11), et de l'article 7 du règlement (UE) 2016/679.

Lorsque le consentement donné aux fins du premier alinéa a été refusé ou retiré par l'utilisateur final, le contrôleur d'accès ne réitère pas sa demande de consentement pour la même finalité plus d'une fois par période d'un an.

Le présent paragraphe est sans préjudice de la possibilité pour le contrôleur d'accès de se fonder sur l'article 6, paragraphe 1, points c), d) et e), du règlement (UE) 2016/679, le cas échéant.

3. Le contrôleur d'accès n'empêche pas les entreprises utilisatrices de proposer les mêmes produits ou services aux utilisateurs finaux au moyen de services d'intermédiation en ligne tiers ou de leur propre canal de vente directe en ligne à des prix ou conditions différents de ceux qui sont proposés par les services d'intermédiation en ligne du contrôleur d'accès.

4. Le contrôleur d'accès permet aux entreprises utilisatrices de communiquer et de promouvoir leurs offres gratuitement, y compris à des conditions différentes, auprès des utilisateurs finaux acquis grâce à son service de plateforme essentiel ou via d'autres canaux, 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.

5. Le contrôleur d'accès permet aux utilisateurs finaux, par l'intermédiaire de ses services de plateforme essentiels, 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, y compris lorsque ces utilisateurs finaux ont acquis de tels éléments auprès des entreprises

utilisatrices concernées sans avoir recours aux services de plateforme essentiels du contrôleur d'accès.

6. Le contrôleur d'accès n'empêche ni ne restreint directement ou indirectement la possibilité pour les entreprises utilisatrices ou les utilisateurs finaux de faire part à toute autorité publique compétente, y compris les juridictions nationales, de tout problème de non-respect, par le contrôleur d'accès, du droit de l'Union ou national pertinent dans le cadre des pratiques de ce dernier. Cela s'entend sans préjudice du droit des entreprises utilisatrices et des contrôleurs d'accès d'établir, dans leurs accords, les conditions d'utilisation de mécanismes légaux de traitement des plaintes.

7. Le contrôleur d'accès n'exige pas des utilisateurs finaux qu'ils utilisent, ni des entreprises utilisatrices qu'elles utilisent, proposent ou interagissent avec un service d'identification, un navigateur internet ou un service de paiement, ou un service technique qui appuie la fourniture des services de paiement, tels que des systèmes de paiement destinés aux achats dans des applications, de ce contrôleur d'accès dans le cadre des services fournis par les entreprises utilisatrices en ayant recours aux services de plateforme essentiels de ce contrôleur d'accès.

8. Le contrôleur d'accès n'exige pas des entreprises utilisatrices ou des utilisateurs finaux qu'ils s'abonnent ou s'enregistrent à tout autre service de plateforme essentiel énuméré dans la décision de désignation conformément à l'article 3, paragraphe 9, ou atteignant les seuils visés à l'article 3, paragraphe 2, point b), comme condition pour être en mesure d'utiliser l'un des services de plateforme essentiels de ce contrôleur d'accès énumérés en vertu dudit article, d'y accéder, de s'y inscrire ou de s'y enregistrer.

9. Le contrôleur d'accès communique quotidiennement à chaque annonceur à qui il fournit des services de publicité en ligne, ou aux tiers autorisés par les annonceurs, à la demande de l'annonceur, des informations gratuites relatives à chaque publicité mise en ligne par l'annonceur, en ce qui concerne:

a)

le prix et les frais payés par cet annonceur, y compris les déductions et suppléments éventuels, pour chacun des services de publicité en ligne concernés fournis par le contrôleur d'accès;

b)

la rémunération perçue par l'éditeur, y compris les déductions et suppléments éventuels, sous réserve du consentement de l'éditeur; et

c)

les mesures quantitatives à partir desquelles chacun des prix, frais et rémunérations est calculé.

Dans le cas où un éditeur ne consent pas au partage d'informations sur la rémunération perçue, comme visé au point b) du premier alinéa, le contrôleur d'accès fournit gratuitement à chaque annonceur des informations sur la rémunération moyenne quotidienne perçue par cet éditeur, y compris les déductions et suppléments éventuels, pour les publicités concernées.

10. Le contrôleur d’accès communique quotidiennement à chaque éditeur à qui il fournit des services de publicité en ligne, ou aux tiers autorisés par les éditeurs, à la demande de l’éditeur, des informations gratuites relatives à chaque publicité affichée dans l’inventaire de l’éditeur, en ce qui concerne:

a)

la rémunération perçue et les frais payés par cet éditeur, y compris les déductions et suppléments éventuels, pour chacun des services de publicité en ligne concernés fournis par le contrôleur d’accès;

b)

le prix payé par l’annonceur, y compris les déductions et suppléments éventuels, sous réserve du consentement de l’annonceur; et

c)

la mesure à partir de laquelle chacun des prix, frais et rémunérations est calculé.

Dans le cas où un annonceur ne consent pas au partage d’informations, le contrôleur d’accès fournit gratuitement à chaque éditeur des informations sur le prix moyen quotidien payé par cet annonceur, y compris les déductions et suppléments éventuels, pour les publicités concernées.

Article 6

Obligations incombant aux contrôleurs d’accès susceptibles d’être précisées en vertu de l’article 8

1. Le contrôleurs d’accès se conforme à toutes les obligations énoncées au présent article pour chacun de ses services de plateforme essentiels énumérés dans la décision de désignation conformément à l’article 3, paragraphe 9.

2. 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.

Aux fins du premier alinéa, les données qui ne sont pas accessibles au public comprennent toutes les données agrégées et non agrégées générées par les entreprises utilisatrices qui peuvent être déduites ou collectées au travers des activités commerciales de ces entreprises ou de leurs clients, y compris les données concernant les clics, les recherches, les vues et la voix, dans le cadre des services de plateforme essentiels concernés ou de services fournis conjointement aux services de plateforme essentiels concernés du contrôleur d’accès, ou à leur appui.

3. Le contrôleur d’accès autorise et permet techniquement la désinstallation facile par les utilisateurs finaux de toute application logicielle dans son système d’exploitation, sans préjudice de la possibilité pour ce 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.

Le contrôleur d’accès autorise et permet techniquement la modification facile par les utilisateurs finaux des paramètres par défaut de son système d’exploitation, son assistant virtuel et son navigateur internet qui dirigent ou orientent les utilisateurs finaux vers des produits et des services proposés par le contrôleur d’accès. Pour ce faire, il invite notamment les utilisateurs finaux, au moment de leur première utilisation de son moteur de recherche en ligne, son assistant virtuel ou son navigateur internet énuméré dans la décision de désignation conformément à l’article 3, paragraphe 9, à choisir dans une liste des principaux fournisseurs de services disponibles, le moteur de recherche en ligne, assistant virtuel ou navigateur internet vers lequel le système d’exploitation du contrôleur d’accès dirige ou oriente les utilisateurs par défaut, et le moteur de recherche en ligne vers lequel l’assistant virtuel et le navigateur internet du contrôleur d’accès dirige ou oriente les utilisateurs par défaut.

4. Le contrôleur d’accès autorise et permet techniquement l’installation et l’utilisation effective d’applications logicielles ou de boutiques d’applications logicielles de tiers utilisant ou interopérant avec son système d’exploitation, et permet l’accès à ces applications logicielles ou boutiques d’applications logicielles par des moyens autres que les services de plateforme essentiels concernés du contrôleur d’accès. Le cas échéant, le contrôleur d’accès n’empêche pas une application logicielle ou boutique d’application logicielle de tiers téléchargée d’inviter les utilisateurs finaux à choisir s’ils souhaitent utiliser par défaut ladite application logicielle ou boutique d’application logicielle téléchargée. Le contrôleur d’accès permet techniquement aux utilisateurs finaux qui choisissent d’utiliser par défaut ladite application logicielle ou boutique d’application logicielle téléchargée de procéder facilement à ce changement.

Rien n’empêche le contrôleur d’accès de prendre, dans la mesure où elles ne vont pas au-delà de ce qui est strictement nécessaire et proportionné, des mesures visant à 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, à condition que ces mesures soient dûment justifiées par le contrôleur d’accès.

En outre, rien n’empêche le contrôleur d’accès d’appliquer, dans la mesure où elles ne vont pas au-delà de ce qui est strictement nécessaire et proportionné, des mesures et des paramètres autres que les paramètres par défaut permettant aux utilisateurs finaux de protéger efficacement la sécurité en ce qui concerne les applications logicielles ou les boutiques d’applications logicielles de tiers, à condition que ces mesures et paramètres autres que les paramètres par défaut soient dûment justifiés par le contrôleur d’accès.

5. Le contrôleur d’accès n’accorde pas, en matière de classement ainsi que pour l’indexation et l’exploration qui y sont liées, un traitement plus favorable aux services et produits proposés par le contrôleur d’accès lui-même qu’aux services ou produits similaires d’un tiers. Le contrôleur d’accès applique des conditions transparentes, équitables et non discriminatoires à ce classement.

6. Le contrôleur d'accès ne restreint pas techniquement ou d'une autre manière la capacité des utilisateurs finaux de changer d'applications logicielles et de services qui sont accessibles en utilisant les services de plateforme essentiels du contrôleur d'accès et de s'y abonner, y compris en ce qui concerne le choix des services d'accès à l'internet pour les utilisateurs finaux.

7. Le contrôleur d'accès permet gratuitement aux fournisseurs de services et aux fournisseurs de matériel informatique d'interopérer efficacement avec les mêmes caractéristiques matérielles et logicielles auxquelles on accède ou qui sont contrôlées par l'intermédiaire du système d'exploitation ou de l'assistant virtuel énuméré dans la décision de désignation conformément à l'article 3, paragraphe 9, que celles qui sont disponibles pour les services ou le matériel fournis par le contrôleur d'accès, ainsi que d'accéder à ces caractéristiques aux fins de l'interopérabilité. En outre, le contrôleur d'accès permet gratuitement aux entreprises utilisatrices et à d'autres fournisseurs de services fournis conjointement à des services de plateforme essentiels, ou à l'appui de ceux-ci, d'interopérer effectivement avec les mêmes caractéristiques du système d'exploitation, matérielles ou logicielles, que ces caractéristiques fassent partie ou non d'un système d'exploitation, que celles qui sont disponibles pour ce contrôleur d'accès ou que celui-ci utilise dans le cadre de la fourniture de tels services, ainsi que d'accéder à ces caractéristiques aux fins de l'interopérabilité.

Rien n'empêche le contrôleur d'accès de prendre des mesures strictement nécessaires et proportionnées visant à éviter que l'interopérabilité ne compromette l'intégrité du système d'exploitation, de l'assistant virtuel, du matériel informatique ou du logiciel qu'il fournit, à condition que ces mesures soient dûment justifiées par le contrôleur d'accès.

8. Le contrôleur d'accès fournit aux annonceurs et aux éditeurs, ainsi qu'aux tiers autorisés par les annonceurs et les éditeurs, à leur demande et gratuitement, un accès aux outils de mesure de performance du contrôleur d'accès et aux données qui leur sont nécessaires pour effectuer leur propre vérification indépendante de l'inventaire publicitaire, notamment les données agrégées et non agrégées. Ces données sont fournies de manière à permettre aux annonceurs et aux éditeurs d'utiliser leurs propres outils de vérification et de mesure afin d'évaluer la performance des services de plateforme essentiels fournis par le contrôleur d'accès.

9. Le contrôleur d'accès assure aux utilisateurs finaux et aux tiers autorisés par un utilisateur final, à leur demande et gratuitement, la portabilité effective des données fournies par l'utilisateur final ou générées par l'activité de l'utilisateur final dans le cadre de l'utilisation du service de plateforme essentiel concerné, y compris en fournissant gratuitement des outils facilitant l'exercice effectif de cette portabilité des données, et notamment en octroyant un accès continu et en temps réel à ces données.

10. Le contrôleur d'accès assure gratuitement aux entreprises utilisatrices et aux tiers autorisés par les entreprises utilisatrices, à leur demande, un accès et une utilisation effectifs, de haute qualité, continus et en temps réel en ce qui concerne les données agrégées et non agrégées, y compris les données à caractère personnel, fournies ou générées dans le cadre de l'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, par ces entreprises utilisatrices et par les utilisateurs finaux qui se servent des produits et services fournis par ces entreprises utilisatrices. En ce qui concerne les données à caractère personnel, le contrôleur d'accès ne donne un tel accès aux données à caractère personnel et ne les utilise

que lorsque les données sont directement liées à l'utilisation faite par les utilisateurs finaux en lien avec les produits ou services que l'entreprise utilisatrice concernée fournit par l'intermédiaire du service de plateforme essentiel concerné, et lorsque les utilisateurs finaux optent pour un tel partage de données en donnant leur consentement.

11. Le contrôleur d'accès procure à toute entreprise tierce fournissant des moteurs de recherche en ligne, à sa demande et à des conditions équitables, raisonnables et non discriminatoires, un accès aux données concernant les classements, requêtes, clics et vues en lien avec les recherches gratuites et payantes générées par les utilisateurs finaux sur ses moteurs de recherche en ligne. Toutes ces données concernant les requêtes, clics et vues constituent des données à caractère personnel et sont anonymisées.

12. Le 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.

La Commission évalue si les conditions générales d'accès publiées sont conformes au présent paragraphe.

13. Le contrôleur d'accès ne dispose pas de conditions générales de résiliation de la fourniture d'un service de plateforme essentiel qui soient disproportionnées. Le contrôleur d'accès veille à ce que les conditions de résiliation puissent être appliquées sans difficulté excessive.

Article 7

Obligations incombant aux contrôleurs d'accès concernant l'interopérabilité des services de communications interpersonnelles non fondés sur la numérotation

1. Lorsqu'un contrôleur d'accès fournit des services de communications interpersonnelles non fondés sur la numérotation qui sont énumérés dans la décision de désignation conformément à l'article 3, paragraphe 9, il rend les fonctionnalités de base de ses services de communications interpersonnelles non fondés sur la numérotation interopérables avec les services de communications interpersonnelles non fondés sur la numérotation de tout autre fournisseur qui propose ou a l'intention de proposer de tels services dans l'Union, en fournissant sur demande et gratuitement les interfaces techniques nécessaires ou des solutions similaires qui facilitent l'interopérabilité.

2. Le contrôleur d'accès rend interopérables au moins les fonctionnalités de base visées au paragraphe 1 énumérées ci-après dès lors qu'il fournit lui-même ces fonctionnalités à ses propres utilisateurs finaux:

a)

à la suite de l'établissement de la liste figurant dans la décision de désignation conformément à l'article 3, paragraphe 9:

i)

messagerie textuelle de bout en bout entre deux utilisateurs finaux individuels;

ii)

partage d'images, de messages vocaux, de vidéos et d'autres fichiers joints dans les communications de bout en bout entre deux utilisateurs finaux individuels;

b)

dans un délai de deux ans à compter de la désignation:

i)

messagerie textuelle de bout en bout entre des groupes d'utilisateurs finaux individuels;

ii)

partage d'images, de messages vocaux, de vidéos et d'autres fichiers joints dans les communications de bout en bout entre une conversation de groupe et un utilisateur final individuel;

c)

dans un délai de quatre ans à compter de la désignation:

i)

appels vocaux de bout en bout entre deux utilisateurs finaux individuels;

ii)

appels vidéo de bout en bout entre deux utilisateurs finaux individuels;

iii)

appels vocaux de bout en bout entre une conversation de groupe et un utilisateur final individuel;

iv)

appels vidéo de bout en bout entre une conversation de groupe et un utilisateur final individuel.

3. Le niveau de sécurité, y compris le chiffrement de bout en bout, le cas échéant, que le contrôleur d'accès fournit à ses propres utilisateurs finaux est maintenu dans l'ensemble des services interopérables.

4. Le contrôleur d’accès publie une offre de référence énonçant les détails techniques et les conditions générales d’interopérabilité avec ses services de communications interpersonnelles non fondés sur la numérotation, y compris les détails nécessaires concernant le niveau de sécurité et le chiffrement de bout en bout. Le contrôleur d’accès publie cette offre de référence avant la fin de la période visée à l’article 3, paragraphe 10, et la met à jour si nécessaire.

5. À la suite de la publication de l’offre de référence conformément au paragraphe 4, tout fournisseur de services de communications interpersonnelles non fondés sur la numérotation qui propose ou a l’intention de proposer de tels services dans l’Union peut demander l’interopérabilité avec les services de communications interpersonnelles non fondés sur la numérotation fournis par le contrôleur d’accès. Une telle demande peut porter sur tout ou partie des fonctionnalités de base énumérées au paragraphe 2. Le contrôleur d’accès accepte toute demande raisonnable d’interopérabilité dans un délai de trois mois à compter de la réception de cette demande en rendant opérationnelles les fonctionnalités de base demandées.

6. La Commission peut, à titre exceptionnel et sur demande motivée du contrôleur d’accès, reporter les délais prévus pour se conformer au paragraphe 2 ou 5 lorsque le contrôleur d’accès démontre que cela est nécessaire pour assurer l’interopérabilité effective et maintenir le niveau de sécurité requis, y compris le chiffrement de bout en bout, le cas échéant.

7. Les utilisateurs finaux des services de communications interpersonnelles non fondés sur la numérotation du contrôleur d’accès et du fournisseur de services de communications interpersonnelles non fondés sur la numérotation qui formule la demande demeurent libres de décider s’ils utilisent les fonctionnalités de base interopérables qui peuvent être fournies par le contrôleur d’accès au titre du paragraphe 1.

8. Le contrôleur d’accès recueille et échange avec le fournisseur de services de communications interpersonnelles non fondés sur la numérotation qui formule une demande d’interopérabilité uniquement les données à caractère personnel d’utilisateurs finaux qui sont strictement nécessaires à la fourniture d’une interopérabilité effective. Toute collecte et tout échange de données à caractère personnel de ce type sont pleinement conformes au règlement (UE) 2016/679 et à la directive 2002/58/CE.

9. Rien n’empêche le contrôleur d’accès de prendre des mesures visant à éviter que les demandes d’interopérabilité formulées par des fournisseurs tiers de services de communications interpersonnelles non fondés sur la numérotation ne compromettent l’intégrité, la sécurité et la confidentialité de ses services, à condition que ces mesures soient strictement nécessaires et proportionnées, et soient dûment justifiées par le contrôleur d’accès.

Article 8

Respect des obligations incombant aux contrôleurs d’accès

1. Le contrôleur d’accès assure et démontre le respect des obligations prévues aux articles 5, 6 et 7 du présent règlement. Les mesures que le contrôleur d’accès met en œuvre pour garantir la conformité avec lesdits articles atteignent effectivement les objectifs du présent règlement et de l’obligation concernée. Le contrôleur d’accès veille à ce que la mise en œuvre de ces mesures respecte le droit applicable, en particulier le règlement (UE) 2016/679, la directive

2002/58/CE, la législation relative à la cybersécurité, à la protection des consommateurs et à la sécurité des produits, ainsi que les exigences en matière d'accessibilité.

2. La Commission peut, de sa propre initiative ou à la demande d'un contrôleur d'accès conformément au paragraphe 3 du présent article, ouvrir la procédure prévue à l'article 20.

La Commission peut adopter un acte d'exécution, qui précise les mesures que le contrôleur d'accès concerné est tenu de mettre en œuvre afin de se conformer effectivement aux obligations énoncées aux articles 6 et 7. Cet acte d'exécution est adopté dans les six mois suivant l'ouverture de la procédure prévue à l'article 20, en conformité avec la procédure consultative visée à l'article 50, paragraphe 2.

Lorsqu'elle ouvre la procédure de sa propre initiative, en cas de contournement, conformément à l'article 13, ces mesures peuvent porter sur les obligations énoncées aux articles 5, 6 et 7.

3. Un contrôleur d'accès peut demander à la Commission d'engager un processus afin de déterminer si les mesures que ce contrôleur d'accès entend mettre en œuvre ou a mises en œuvre pour se conformer aux articles 6 et 7 atteignent effectivement l'objectif de l'obligation pertinente dans la situation spécifique du contrôleur d'accès. La Commission dispose d'une marge d'appréciation pour décider s'il y a lieu d'engager un tel processus, dans le respect des principes d'égalité de traitement, de proportionnalité et de bonne administration.

Dans sa demande, le contrôleur d'accès fournit un mémoire motivé pour expliquer les mesures qu'il entend mettre en œuvre ou a mises en œuvre. Le contrôleur d'accès fournit en outre une version non confidentielle de son mémoire motivé qui peut être partagée avec des tiers conformément au paragraphe 6.

4. Les paragraphes 2 et 3 sont sans préjudice des pouvoirs conférés à la Commission en vertu des articles 29, 30 et 31.

5. En vue de l'adoption de la décision visée au paragraphe 2, la Commission fait part de ses constatations préliminaires au contrôleur d'accès dans un délai de trois mois à compter de l'ouverture de la procédure au titre de l'article 20. Dans ses constatations préliminaires, la Commission explique les mesures qu'elle envisage de prendre ou que le contrôleur d'accès concerné devrait prendre, selon elle, afin de donner suite de manière effective aux constatations préliminaires.

6. Afin de permettre effectivement aux tiers intéressés de présenter des observations, la Commission publie, lorsqu'elle communique ses constatations préliminaires au contrôleur d'accès conformément au paragraphe 5 ou le plus tôt possible après une telle communication, une synthèse non confidentielle de la situation et les mesures qu'elle envisage de prendre ou que le contrôleur d'accès concerné devrait prendre selon elle. La Commission fixe un délai raisonnable dans lequel ces observations peuvent être formulées.

7. En précisant les mesures visées au paragraphe 2, la Commission veille à ce qu'elles atteignent effectivement les objectifs du présent règlement et de l'obligation pertinente et à ce qu'elles soient proportionnées compte tenu de la situation spécifique du contrôleur d'accès et du service concerné.

8. Dans le but de préciser les obligations prévues à l'article 6, paragraphes 11 et 12, la Commission évalue en outre si les mesures envisagées ou mises en œuvre garantissent qu'aucun déséquilibre ne demeure entre les droits et les obligations des entreprises utilisatrices et si les mesures ne confèrent pas elles-mêmes au contrôleur d'accès un avantage disproportionné par rapport au service qu'il fournit aux entreprises utilisatrices.

9. En ce qui concerne la procédure visée au paragraphe 2, la Commission peut, sur demande ou de sa propre initiative, décider de la rouvrir lorsque:

a)

l'un des faits sur lesquels la décision repose subit un changement important; ou

b)

la décision repose sur des informations incomplètes, inexactes ou dénaturées; ou

c)

les mesures énoncées dans la décision ne sont pas efficaces.

Article 9

Suspension

1. Lorsque le contrôleur d'accès démontre dans une demande motivée que le respect d'une obligation spécifique énoncée à l'article 5, 6 ou 7 concernant un service de plateforme essentiel énuméré dans la décision de désignation conformément à l'article 3, paragraphe 9, menacerait, en raison de circonstances exceptionnelles échappant à son contrôle, la viabilité économique de ses activités dans l'Union, la Commission peut adopter un acte d'exécution établissant sa décision de suspendre, à titre exceptionnel, entièrement ou partiellement, l'obligation spécifique visée dans cette demande motivée (ci-après dénommée «décision de suspension»). Dans cet acte d'exécution, la Commission étaye sa décision de suspension en indiquant les circonstances exceptionnelles justifiant la suspension. La portée et la durée de cet acte d'exécution sont limitées à ce qui est nécessaire pour remédier à cette menace pour la viabilité du contrôleur d'accès. La Commission s'efforce d'adopter cet acte d'exécution sans tarder et au plus tard trois mois après réception d'une demande complète et motivée. Cet acte d'exécution est adopté en conformité avec la procédure consultative visée à l'article 50, paragraphe 2.

2. Lorsqu'une suspension est accordée en vertu du paragraphe 1, la Commission réexamine sa décision de suspension chaque année, à moins qu'un intervalle plus court ne soit indiqué dans ladite décision. À la suite de ce réexamen, la Commission lève entièrement ou partiellement la suspension, ou décide que les conditions visées au paragraphe 1 demeurent remplies.

3. En cas d'urgence, sur demande motivée d'un contrôleur d'accès, la Commission peut suspendre provisoirement l'application d'une obligation spécifique visée au paragraphe 1 pour un ou plusieurs services de plateforme essentiels spécifiques, avant même d'adopter la

décision visée audit paragraphe. Une telle demande peut être présentée et acceptée à tout moment, dans l'attente de l'évaluation de la Commission en application du paragraphe 1.

4. Lors de l'évaluation de la demande visée aux paragraphes 1 et 3, la Commission tient compte en particulier de l'incidence du respect de l'obligation spécifique sur la viabilité économique des activités du contrôleur d'accès dans l'Union ainsi que sur les tiers, en particulier les PME et les consommateurs. La suspension peut être soumise à des conditions et obligations devant être définies par la Commission afin de garantir un juste équilibre entre ces intérêts et les objectifs du présent règlement.

Article 10

Exemption pour raisons de santé publique et de sécurité publique

1. Sur demande motivée d'un contrôleur d'accès ou de sa propre initiative, la Commission peut adopter un acte d'exécution établissant sa décision d'exempter ce contrôleur d'accès, entièrement ou partiellement, d'une obligation particulière prévue à l'article 5, 6 ou 7 en ce qui concerne un service de plateforme essentiel énuméré dans la décision de désignation conformément à l'article 3, paragraphe 9, lorsqu'une telle exemption est justifiée par les motifs énoncés au paragraphe 3 du présent article (ci-après dénommée «décision d'exemption»). La Commission adopte la décision d'exemption dans un délai de trois mois après réception d'une demande complète et motivée, et fournit une déclaration motivée expliquant les raisons de l'exemption. Cet acte d'exécution est adopté en conformité avec la procédure consultative visée à l'article 50, paragraphe 2.

2. Lorsqu'une exemption est accordée en vertu du paragraphe 1, la Commission réexamine sa décision d'exemption lorsque le motif de l'exemption n'existe plus ou au minimum chaque année. À la suite de ce réexamen, la Commission lève entièrement ou partiellement l'exemption ou décide que les conditions du paragraphe 1 demeurent remplies.

3. Une exemption en vertu du paragraphe 1 ne peut être accordée que pour des motifs de santé publique ou de sécurité publique.

4. En cas d'urgence, sur demande motivée d'un contrôleur d'accès ou de sa propre initiative, la Commission peut suspendre provisoirement l'application d'une obligation spécifique visée au paragraphe 1 pour un ou plusieurs services de plateforme essentiels spécifiques, avant même d'adopter la décision visée audit paragraphe. Une telle demande peut être présentée et acceptée à tout moment, dans l'attente de l'évaluation de la Commission en application du paragraphe 1.

5. Lors de l'évaluation de la demande visée aux paragraphes 1 et 4, la Commission tient compte en particulier de l'incidence du respect de l'obligation spécifique sur les motifs énumérés au paragraphe 3, ainsi que des effets sur le contrôleur d'accès concerné et sur les tiers. La Commission peut soumettre la suspension à des conditions et obligations afin de garantir un juste équilibre entre les objectifs visés par les motifs énoncés au paragraphe 3 et les objectifs du présent règlement.

Article 11

Établissement de rapports

1. Dans les six mois suivant sa désignation au titre de l'article 3, et conformément à l'article 3, paragraphe 10, le contrôleur d'accès remet à la Commission un rapport décrivant de manière détaillée et transparente les mesures qu'il a mises en œuvre pour garantir le respect des obligations énoncées aux articles 5, 6 et 7.

2. Dans le délai visé au paragraphe 1, le contrôleur d'accès publie et remet à la Commission une synthèse non confidentielle de ce rapport.

Le contrôleur d'accès met à jour au moins annuellement ce rapport et cette synthèse non confidentielle.

La Commission insère sur son site internet un lien vers cette synthèse non confidentielle.

Article 12

Mise à jour des obligations des contrôleurs d'accès

1. La Commission est habilitée à adopter des actes délégués conformément à l'article 49 pour compléter le présent règlement en ce qui concerne les obligations existantes énoncées aux articles 5 et 6. Ces actes délégués sont fondés sur une enquête de marché menée en vertu de l'article 19 qui a mis en évidence la nécessité de maintenir à jour ces obligations afin de lutter contre les pratiques qui limitent la contestabilité des services de plateforme essentiels ou qui sont déloyales au même titre que les pratiques qui sont l'objet des obligations énoncées aux articles 5 et 6.

2. Le champ d'application d'un acte délégué adopté conformément au paragraphe 1 se limite à:

a)

élargir une obligation qui s'applique uniquement dans le cadre de certains services de plateforme essentiels à d'autres services de plateforme essentiels énumérés à l'article 2, point 2);

b)

élargir une obligation dont bénéficient certaines entreprises utilisatrices ou utilisateurs finaux de manière à ce que d'autres entreprises utilisatrices ou utilisateurs finaux en soient bénéficiaires;

c)

préciser les modalités d'exécution par les contrôleurs d'accès des obligations énoncées aux articles 5 et 6 afin de garantir le respect effectif de ces obligations;

d)

élargir une obligation qui s’applique uniquement dans le cadre de certains services fournis conjointement à des services de plateforme essentiels, ou à leur appui, à d’autres services fournis conjointement à des services de plateforme essentiels, ou à leur appui;

e)

élargir une obligation qui s’applique uniquement dans le cadre de certains types de données afin qu’elle s’applique à d’autres types de données;

f)

ajouter des conditions supplémentaires lorsqu’une obligation impose certaines conditions concernant le comportement d’un contrôleur d’accès; ou

g)

appliquer une obligation qui régit la relation entre plusieurs services de plateforme essentiels du contrôleur d’accès à la relation entre un service de plateforme essentiel et d’autres services du contrôleur d’accès.

3. La Commission est habilitée à adopter des actes délégués conformément à l’article 49 pour modifier le présent règlement en ce qui concerne la liste des fonctionnalités de base recensées à l’article 7, paragraphe 2, en ajoutant ou en supprimant des fonctionnalités de services de communications interpersonnelles non fondés sur la numérotation.

Ces actes délégués sont fondés sur une enquête de marché menée en vertu de l’article 19 qui a mis en évidence la nécessité de maintenir à jour ces obligations afin de lutter contre les pratiques qui limitent la contestabilité des services de plateforme essentiels ou qui sont déloyales au même titre que les pratiques qui sont l’objet des obligations énoncées à l’article 7.

4. La Commission est habilitée à adopter des actes délégués conformément à l’article 49 pour compléter le présent règlement en ce qui concerne les obligations prévues à l’article 7 en précisant les modalités d’exécution des obligations afin de garantir le respect effectif de ces obligations. Ces actes délégués sont fondés sur une enquête de marché menée en vertu de l’article 19 qui a mis en évidence la nécessité de maintenir à jour ces obligations afin de lutter contre les pratiques qui limitent la contestabilité des services de plateforme essentiels ou qui sont déloyales au même titre que les pratiques qui sont l’objet des obligations énoncées à l’article 7.

5. Une pratique visée aux paragraphes 1, 3 et 4 est considérée comme limitant la contestabilité des services de plateforme essentiels ou comme déloyale:

a)

lorsque cette pratique est le fait des contrôleurs d’accès et est susceptible d’entraver l’innovation et de limiter le choix pour les entreprises utilisatrices et les utilisateurs finaux parce qu’elle:

i)

porte atteinte ou risque de porter atteinte durablement à la contestabilité d'un service de plateforme essentiel ou d'autres services dans le secteur numérique en raison de la création ou du renforcement d'obstacles empêchant d'autres entreprises de s'implanter ou de se développer en tant que fournisseurs d'un service de plateforme essentiel ou d'autres services dans le secteur numérique; ou

ii)

empêche les autres opérateurs d'avoir le même accès que le contrôleur d'accès à un intrant clé; ou

b)

lorsqu'il existe un déséquilibre entre les droits et les obligations des entreprises utilisatrices et que le contrôleur d'accès obtient un avantage des entreprises utilisatrices qui est disproportionné par rapport au service fourni par ce contrôleur d'accès à ces entreprises utilisatrices.

Article 13

Anticontournement

1. Une entreprise fournissant des services de plateforme essentiels ne segmente pas, ni ne divise, subdivise, fragmente ou fractionne ces services par des moyens contractuels, commerciaux, techniques ou autres dans le but de contourner les seuils quantitatifs fixés à l'article 3, paragraphe 2. Aucune de ces pratiques de la part d'une entreprise n'empêche la Commission de désigner celle-ci comme contrôleur d'accès au titre de l'article 3, paragraphe 4.

2. Lorsqu'elle soupçonne qu'une entreprise fournissant des services de plateforme essentiels met en œuvre une pratique visée au paragraphe 1, la Commission peut exiger de cette entreprise toute information qu'elle juge nécessaire pour déterminer si cette entreprise s'est livrée à une telle pratique.

3. Le contrôleur d'accès veille à ce que les obligations des articles 5, 6 et 7 soient pleinement et effectivement respectées.

4. Le contrôleur d'accès ne se livre à aucun comportement compromettant le respect effectif des obligations des articles 5, 6 et 7, que ce comportement soit de nature contractuelle, commerciale, technique ou autre, ou qu'il consiste en l'utilisation de techniques comportementales ou d'une conception d'interface.

5. Si le consentement est requis pour la collecte, le traitement, l'utilisation croisée et le partage de données à caractère personnel afin que le respect du présent règlement soit garanti, le contrôleur d'accès prend les mesures nécessaires, soit pour permettre aux entreprises utilisatrices d'obtenir directement le consentement requis au traitement de ces données, lorsque ce consentement est exigé en application du règlement (UE) 2016/679 ou de la directive 2002/58/CE, soit pour se conformer aux règles et principes de l'Union en matière de protection des données et de la vie privée par d'autres moyens, dont la fourniture aux

entreprises utilisatrices de données dûment anonymisées, s'il y a lieu. Le contrôleur d'accès ne rend pas l'obtention de ce consentement par les entreprises utilisatrices plus lourde que pour ses propres services.

6. Le contrôleur d'accès ne détériore ni les conditions, ni la qualité de l'un de ses services de plateforme essentiels fournis aux entreprises utilisatrices ou aux utilisateurs finaux qui font valoir leurs droits ou choix prévus aux articles 5, 6 et 7, et ne rend pas l'exercice de ces droits ou choix excessivement difficile, y compris en proposant des choix à l'utilisateur final de manière partiale, ou encore en utilisant la structure, la conception, la fonction ou le mode de fonctionnement d'une interface utilisateur ou d'une partie connexe pour perturber l'autonomie des utilisateurs finaux ou des entreprises utilisatrices, leur prise de décision ou leur libre choix.

7. Lorsque le contrôleur d'accès contourne ou tente de contourner l'une des obligations énoncées à l'article 5, 6 ou 7 d'une manière décrite aux paragraphes 4, 5 et 6 du présent article, la Commission peut ouvrir la procédure prévue à l'article 20 et adopter un acte d'exécution visé à l'article 8, paragraphe 2, afin de préciser les mesures que le contrôleur d'accès est tenu de mettre en œuvre.

8. Le paragraphe 6 du présent article est sans préjudice des pouvoirs conférés à la Commission en vertu des articles 29, 30 et 31.

Article 14

Obligation d'informer sur les concentrations

1. Le contrôleur d'accès informe la Commission de tout projet de concentration au sens de l'article 3 du règlement (CE) no 139/2004, lorsque les entités qui fusionnent ou la cible de la concentration fournissent des services de plateforme essentiels ou tout autre service dans le secteur numérique ou permettent la collecte de données, que ce projet soit soumis à une obligation de notification à la Commission en application dudit règlement ou à une autorité nationale de concurrence compétente selon les règles nationales en matière de concentrations.

Le contrôleur d'accès informe la Commission de cette concentration avant sa réalisation et après la conclusion de l'accord, la publication de l'offre publique d'achat ou d'échange ou l'acquisition d'une participation de contrôle.

2. Les informations communiquées par le contrôleur d'accès conformément au paragraphe 1 renseignent au moins sur les entreprises concernées par la concentration, leurs chiffres d'affaires annuels mondiaux et au sein de l'Union, leurs domaines d'activité, y compris les activités directement liées à la concentration et la valeur transactionnelle de l'accord ou une estimation de celle-ci, et sont accompagnées d'un résumé relatif à la concentration, y compris sa nature et sa justification, et d'une liste des États membres concernés par la concentration.

Les informations communiquées par le contrôleur d'accès indiquent également, pour tous les services de plateforme essentiels concernés, leurs chiffres d'affaires annuels au sein de l'Union, le nombre d'entreprises utilisatrices actives par an et le nombre d'utilisateurs finaux actifs par mois, respectivement.

3. Si à la suite d'une concentration visée au paragraphe 1 du présent article, d'autres services de plateforme essentiels atteignent, individuellement, les seuils fixés à l'article 3, paragraphe 2, point b), le contrôleur d'accès concerné en informe la Commission dans les deux mois à compter de la réalisation de la concentration et fournit à la Commission les informations visées à l'article 3, paragraphe 2.

4. La Commission communique aux autorités compétentes des États membres toute information reçue en application du paragraphe 1 et publie chaque année la liste des acquisitions dont elle a été informée par les contrôleurs d'accès en application dudit paragraphe.

La Commission tient compte de l'intérêt légitime des entreprises à ce que leurs secrets d'affaires ne soient pas divulgués.

5. Les autorités compétentes des États membres peuvent utiliser les informations reçues au titre du paragraphe 1 du présent article pour demander à la Commission d'examiner la concentration conformément à l'article 22 du règlement (CE) no 139/2004.

Article 15

Obligation d'audit

1. Dans les six mois suivant sa désignation conformément à l'article 3, le contrôleur d'accès soumet à la Commission une description ayant fait l'objet d'un audit indépendant de toutes les techniques de profilage des consommateurs qu'il applique dans le cadre de ses services de plateforme essentiels énumérés dans la décision de désignation conformément à l'article 3, paragraphe 9. La Commission transmet cette description ayant fait l'objet d'un audit au comité européen de la protection des données.

2. La Commission peut adopter un acte d'exécution visé à l'article 46, paragraphe 1, point g), afin de mettre au point la méthodologie et la procédure de l'audit.

3. Le contrôleur d'accès met à la disposition du public un aperçu de la description ayant fait l'objet d'un audit visée au paragraphe 1. Ce faisant, le contrôleur d'accès est autorisé à tenir compte de la nécessité que ses secrets d'affaires ne soient pas divulgués. Le contrôleur d'accès met à jour au moins annuellement cette description et cet aperçu.

CHAPITRE IV

ENQUÊTE DE MARCHÉ

Article 16

Ouverture d'une enquête de marché

1. Lorsque la Commission a l'intention de mener une enquête de marché en vue de l'adoption éventuelle de décisions en vertu des articles 17, 18 et 19, elle adopte une décision relative à l'ouverture d'une enquête de marché.

2. Nonobstant le paragraphe 1, la Commission peut exercer ses pouvoirs d'enquête en vertu du présent règlement avant d'ouvrir une enquête de marché conformément audit paragraphe.

3. La décision visée au paragraphe 1 précise:

a)

la date d'ouverture de l'enquête de marché;

b)

la description de la question sur laquelle porte l'enquête de marché;

c)

le but de l'enquête de marché.

4. La Commission peut rouvrir une enquête de marché qu'elle a clôturée si:

a)

l'un des faits sur lesquels repose une décision adoptée en vertu de l'article 17, 18 ou 19 subit un changement important; ou

b)

la décision adoptée en vertu de l'article 17, 18 ou 19 repose sur des renseignements incomplets, inexacts ou dénaturés.

5. La Commission peut demander à une ou plusieurs autorités nationales compétentes de l'assister dans son enquête de marché.

Article 17

Enquête de marché pour la désignation des contrôleurs d'accès

1. La Commission peut mener une enquête de marché afin d'examiner si une entreprise fournissant des services de plateforme essentiels devrait être désignée comme étant un contrôleur d'accès en vertu de l'article 3, paragraphe 8, ou aux fins de déterminer les services de plateforme essentiels devant être recensés dans la décision de désignation en vertu de l'article 3, paragraphe 9. La Commission s'efforce de conclure son enquête de marché dans un délai de douze mois à compter de la date visée à l'article 16, paragraphe 3, point a). Afin de conclure son enquête de marché, la Commission adopte un acte d'exécution énonçant sa décision. Cet acte d'exécution est adopté en conformité avec la procédure consultative visée à l'article 50, paragraphe 2.

2. Au cours d'une enquête de marché menée en vertu du paragraphe 1 du présent article, la Commission s'efforce de communiquer ses constatations préliminaires à l'entreprise fournissant des services de plateforme essentiels concernée, dans un délai de six mois à compter de la date visée à l'article 16, paragraphe 3, point a). Dans ses constatations

préliminaires, la Commission explique si elle estime, à titre provisoire, qu'il est approprié que ladite entreprise soit désignée comme contrôleur d'accès en vertu de l'article 3, paragraphe 8, et que les services de plateforme essentiels concernés soient énumérés conformément à l'article 3, paragraphe 9.

3. Lorsque l'entreprise fournissant des services de plateforme essentiels atteint les seuils fixés à l'article 3, paragraphe 2, mais qu'elle a présenté des arguments suffisamment étayés en vertu de l'article 3, paragraphe 5, qui ont manifestement remis en cause la présomption énoncée à l'article 3, paragraphe 2, la Commission s'efforce de conclure l'enquête de marché dans un délai de cinq mois à compter de la date visée à l'article 16, paragraphe 3, point a).

Dans un tel cas, la Commission s'efforce de communiquer à l'entreprise concernée ses constatations préliminaires conformément au paragraphe 2 du présent article dans un délai de trois mois à compter de la date visée à l'article 16, paragraphe 3, point a).

4. Lorsque la Commission, en vertu de l'article 3, paragraphe 8, désigne comme contrôleur d'accès une entreprise fournissant des services de plateforme essentiels qui ne jouit pas encore d'une position solide et durable dans ses activités, mais en jouira de manière prévisible dans un avenir proche, elle peut ne déclarer applicable à ce contrôleur d'accès qu'une ou plusieurs des obligations énoncées à l'article 5, paragraphes 3 à 6, et à l'article 6, paragraphes 4, 7, 9, 10 et 13, telles qu'elles sont précisées dans la décision de désignation. La Commission ne déclare applicables que les obligations appropriées et nécessaires pour empêcher le contrôleur d'accès concerné d'acquérir, par des moyens déloyaux, une position solide et durable dans ses activités. La Commission réexamine cette désignation conformément à la procédure prévue à l'article 4.

Article 18

Enquête de marché portant sur un non-respect systématique

1. La Commission peut mener une enquête de marché afin d'examiner si un contrôleur d'accès a fait preuve d'un non-respect systématique. La Commission conclut cette enquête de marché dans un délai de douze mois à compter de la date visée à l'article 16, paragraphe 3, point a). Lorsqu'il ressort de l'enquête de marché qu'un contrôleur d'accès a systématiquement contrevenu à une ou plusieurs des obligations prévues à l'article 5, 6 ou 7 et qu'il a maintenu, renforcé ou étendu sa position de contrôleur d'accès au regard des caractéristiques énoncées à l'article 3, paragraphe 1, la Commission peut adopter un acte d'exécution imposant à un tel contrôleur d'accès toute mesure corrective comportementale ou structurelle qui soit proportionnée et nécessaire pour garantir le respect effectif du présent règlement. Cet acte d'exécution est adopté en conformité avec la procédure consultative visée à l'article 50, paragraphe 2.

2. La mesure corrective imposée conformément au paragraphe 1 du présent article peut inclure, dans la mesure où cette mesure corrective est proportionnée et nécessaire pour préserver ou rétablir l'équité et la contestabilité affectées par le non-respect systématique, l'interdiction faite au contrôleur d'accès, pendant une période limitée, de se lancer dans une concentration au sens de l'article 3 du règlement (CE) no 139/2004 en ce qui concerne les services de plateforme essentiels ou d'autres services fournis dans le secteur numérique ou permettant la collecte de données, qui sont affectés par le non-respect systématique.

3. Un contrôleur d’accès est réputé avoir systématiquement contrevenu aux obligations prévues aux articles 5, 6 et 7 lorsque la Commission a émis au moins trois décisions constatant un manquement au titre de l’article 29 à l’encontre d’un contrôleur d’accès en ce qui concerne l’un de ses services de plateforme essentiels au cours d’une période de huit ans ayant précédé l’adoption de la décision d’ouverture d’une enquête de marché en vue de l’adoption éventuelle d’une décision selon le présent article.

4. La Commission communique ses constatations préliminaires au contrôleur d’accès concerné dans un délai de six mois à compter de la date visée à l’article 16, paragraphe 3, point a). Dans ses constatations préliminaires, la Commission explique si elle estime, à titre préliminaire, que les conditions prévues au paragraphe 1 du présent article sont réunies et quelle mesure ou quelles mesures correctives elle considère, à titre préliminaire, comme nécessaires et proportionnées.

5. Afin de permettre aux tiers intéressés de formuler effectivement des observations, la Commission publie, en même temps qu’elle communique ses constatations préliminaires au contrôleur d’accès conformément au paragraphe 4 ou le plus tôt possible après une telle communication, une synthèse non confidentielle de l’affaire et des mesures correctives qu’elle envisage d’imposer. La Commission fixe un délai raisonnable dans lequel de telles observations doivent être formulées.

6. Lorsque la Commission a l’intention d’adopter une décision en vertu du paragraphe 1 du présent article en rendant obligatoires les engagements que le contrôleur d’accès propose de prendre en vertu de l’article 25, elle publie une synthèse non confidentielle de l’affaire ainsi que l’essentiel du contenu des engagements. Les tiers intéressés peuvent soumettre leurs observations dans un délai raisonnable qui est fixé par la Commission.

7. Au cours de l’enquête de marché, la Commission peut en prolonger la durée, à condition que cette prolongation se justifie par des motifs objectifs et soit proportionnée. Cette prolongation peut s’appliquer au délai imparti à la Commission pour formuler ses constatations préliminaires ou au délai imparti pour l’adoption de la décision finale. La durée totale de la ou des prolongations décidées en vertu du présent paragraphe ne dépasse pas six mois.

8. Afin de garantir le respect effectif des obligations prévues aux articles 5, 6 et 7 par le contrôleur d’accès, la Commission réexamine régulièrement les mesures correctives qu’elle impose conformément aux paragraphes 1 et 2 du présent article. La Commission est habilitée à modifier ces mesures correctives si, après une nouvelle enquête de marché, elle estime que celles-ci ne sont pas efficaces.

Article 19

Enquête de marché portant sur les nouveaux services et les nouvelles pratiques

1. La Commission peut mener une enquête de marché afin d’examiner s’il conviendrait d’inscrire un ou plusieurs services du secteur numérique sur la liste des services de plateforme essentiels prévus à l’article 2, point 2), ou afin de détecter des pratiques qui limitent la contestabilité des services de plateforme essentiels ou qui sont déloyaux et auxquels le présent règlement ne permet pas de remédier de manière effective. Dans son évaluation, la Commission tient compte de toutes les conclusions pertinentes des procédures au titre des

articles 101 et 102 du traité sur le fonctionnement de l'Union européenne concernant les marchés numériques, ainsi que de toute autre évolution pertinente.

2. La Commission peut, lorsqu'elle mène une enquête de marché en vertu du paragraphe 1, consulter des tiers, y compris des entreprises utilisatrices et des utilisateurs finaux de services du secteur numérique qui font l'objet d'une enquête, ainsi que des entreprises utilisatrices et des utilisateurs finaux soumis à des pratiques faisant l'objet d'une enquête.

3. La Commission publie ses constatations dans un rapport dans un délai de dix-huit mois à compter de la date visée à l'article 16, paragraphe 3, point a).

Ce rapport est présenté au Parlement européen et au Conseil tout en étant, s'il y a lieu, assorti:

a)

d'une proposition législative modifiant le présent règlement dans le but d'inclure des services supplémentaires du secteur numérique dans la liste des services de plateforme essentiels établie à l'article 2, point 2), ou d'intégrer de nouvelles obligations au chapitre III; ou

b)

d'un projet d'acte délégué complétant le présent règlement en ce qui concerne les obligations énoncées aux articles 5 et 6, ou d'un projet d'acte délégué modifiant ou complétant le présent règlement en ce qui concerne les obligations énoncées à l'article 7, comme prévu à l'article 12.

Le cas échéant, la proposition législative modifiant le présent règlement visé au deuxième alinéa, point a), peut également viser à supprimer les services existants de la liste des services de plateforme essentiels établie à l'article 2, point 2), ou à supprimer des obligations existantes de l'article 5, 6 ou 7.

CHAPITRE V

POUVOIRS D'ENQUÊTE, DE COERCITION ET DE CONTRÔLE

Article 20

Ouverture d'une procédure

1. Lorsque la Commission a l'intention d'ouvrir une procédure en vue de l'adoption éventuelle de décisions au titre des articles 8, 29 et 30, elle adopte une décision relative à l'ouverture d'une procédure.

2. Nonobstant le paragraphe 1, la Commission peut exercer ses pouvoirs d'enquête en vertu du présent règlement avant d'ouvrir une procédure conformément audit paragraphe.

Article 21

Demandes de renseignements

1. Pour l'accomplissement de ses tâches au titre du présent règlement, la Commission peut, par simple demande ou par voie de décision, exiger des entreprises et associations d'entreprises qu'elles fournissent tous les renseignements nécessaires. La Commission peut également, par simple demande ou par voie de décision, exiger l'accès à toutes les données et algorithmes des entreprises et à des renseignements concernant les essais, ainsi que demander des explications les concernant.

2. Lorsqu'elle envoie une simple demande de renseignements à une entreprise ou à une association d'entreprises, la Commission indique la base juridique et le but de la demande, précise les renseignements demandés et fixe le délai dans lequel ils doivent être fournis, ainsi que les amendes prévues à l'article 30 qui est d'application au cas où des renseignements ou des explications incomplets, inexacts ou dénaturés seraient fournis.

3. Lorsque la Commission demande, par décision, aux entreprises et associations d'entreprises de fournir des renseignements, elle indique la base juridique et le but de la demande, précise les renseignements demandés et fixe le délai dans lequel les renseignements doivent être fournis. Lorsque la Commission demande aux entreprises de donner accès à toutes les données, tous les algorithmes et à des renseignements concernant les essais, elle indique le but de la demande et fixe le délai dans lequel il doit être accordé. Elle énonce également les amendes prévues à l'article 30 et indique ou inflige les astreintes prévues à l'article 31. De plus, elle informe du droit de faire examiner la décision par la Cour de justice.

4. Les entreprises ou associations d'entreprises ou leurs représentants fournissent les renseignements demandés, au nom de l'entreprise ou de l'association d'entreprises concernées. Les avocats dûment mandatés peuvent fournir les renseignements demandés au nom de leurs mandants. Ces derniers restent pleinement responsables du caractère complet, exact et non dénaturé des renseignements fournis.

5. À la demande de la Commission, les autorités compétentes des États membres fournissent à la Commission tous les renseignements en leur possession qui sont nécessaires à l'accomplissement des tâches qui lui sont assignées par le présent règlement.

Article 22

Pouvoir de mener des auditions et de recueillir des déclarations

1. Pour l'accomplissement de ses tâches au titre du présent règlement, la Commission peut entendre toute personne physique ou morale qui accepte d'être auditionnée, aux fins de la collecte d'informations, en lien avec l'objet d'une enquête. La Commission a le droit d'enregistrer ces auditions par tout moyen technique.

2. Lorsqu'une audition au titre du paragraphe 1 du présent article est menée dans les locaux d'une entreprise, la Commission en informe l'autorité nationale compétente de l'État membre chargée de faire appliquer les règles visées à l'article 1er, paragraphe 6, et sur le territoire duquel l'audition a lieu. Si cette autorité le demande, les agents de celle-ci peuvent prêter assistance aux agents et aux autres personnes les accompagnant mandatés par la Commission pour conduire l'audition.

Article 23

Pouvoirs d’effectuer des inspections

1. Pour l’accomplissement de ses tâches au titre du présent règlement, la Commission peut procéder à toutes les inspections nécessaires d’une entreprise ou d’une association d’entreprises.

2. Les agents et les autres personnes les accompagnant mandatés par la Commission pour procéder à une inspection sont investis des pouvoirs suivants:

a)

accéder à tous les locaux, terrains et moyens de transport des entreprises et associations d’entreprises;

b)

contrôler les livres et autres documents en rapport avec l’activité, quel qu’en soit le support;

c)

prendre ou obtenir sous quelque forme que ce soit copie ou extrait des livres et documents;

d)

exiger de l’entreprise ou de l’association d’entreprises qu’elle donne accès à son organisation, son fonctionnement, son système informatique, ses algorithmes, son traitement des données et ses pratiques commerciales et qu’elle fournisse des explications sur ces différents éléments, et enregistrer ou consigner les explications données par tout moyen technique;

e)

apposer des scellés sur tous les locaux commerciaux et livres ou documents pendant la durée de l’inspection et dans la mesure où cela est nécessaire aux fins de celle-ci;

f)

demander à tout représentant ou membre du personnel de l’entreprise ou de l’association d’entreprises des explications sur des faits ou documents en rapport avec l’objet et le but de l’inspection et enregistrer ses réponses par tout moyen technique.

3. Pour effectuer les inspections, la Commission peut demander le concours d’auditeurs ou d’experts nommés par la Commission en vertu de l’article 26, paragraphe 2, ainsi que celui de l’autorité nationale compétente de l’État membre chargée de faire appliquer les règles visées à l’article 1er, paragraphe 6, sur le territoire duquel l’inspection doit être menée.

4. Au cours des inspections, la Commission, les auditeurs ou experts nommés par cette dernière et l’autorité nationale compétente de l’État membre chargée de faire appliquer les règles visées à l’article 1er, paragraphe 6, sur le territoire duquel l’inspection doit être menée peuvent exiger de l’entreprise ou de l’association d’entreprises qu’elle donne accès à son organisation, son fonctionnement, son système informatique, ses algorithmes, son traitement

des données et ses pratiques commerciales et qu'elle fournisse des explications sur ces différents éléments. La Commission et les auditeurs ou experts nommés par celle-ci et l'autorité nationale compétente de l'État membre chargée de faire appliquer les règles visées à l'article 1er, paragraphe 6, sur le territoire duquel l'inspection doit être menée peuvent poser des questions à tout représentant ou membre du personnel.

5. Les agents et les autres personnes les accompagnant mandatés par la Commission pour procéder à une inspection exercent leurs pouvoirs sur production d'un mandat écrit qui indique l'objet et le but de l'inspection, ainsi que les amendes prévues à l'article 30, qui s'appliquent au cas où les livres ou autres documents professionnels qui sont requis seraient présentés de manière incomplète et où les réponses aux demandes faites en application des paragraphes 2 et 4 du présent article seraient inexactes ou dénaturées. La Commission avise, en temps utile avant l'inspection, l'autorité nationale compétente de l'État membre chargée de faire appliquer les règles visées à l'article 1, paragraphe 6, sur le territoire duquel l'inspection doit être effectuée.

6. Les entreprises ou associations d'entreprises sont tenues de se soumettre à une inspection ordonnée par une décision de la Commission. Cette décision indique l'objet et le but de l'inspection, fixe la date à laquelle elle commence, indique les amendes et astreintes prévues aux articles 30 et 31 respectivement et informe du droit de faire examiner ladite décision devant la Cour de justice.

7. Les agents de l'autorité nationale compétente de l'État membre chargée de faire appliquer les règles visées à l'article 1er, paragraphe 6, sur le territoire duquel l'inspection doit être menée et les personnes mandatées ou nommées par cette autorité prêtent, à la demande de ladite autorité ou de la Commission, un concours actif aux agents et aux autres personnes les accompagnant mandatés par la Commission. Ils disposent à cette fin des pouvoirs prévus aux paragraphes 2 et 4 du présent article.

8. Lorsque les agents ou les autres personnes les accompagnant mandatés par la Commission constatent qu'une entreprise ou une association d'entreprises s'oppose à une inspection ordonnée en vertu du présent article, l'État membre concerné leur prête l'assistance nécessaire, en requérant au besoin la force publique ou une autorité disposant d'un pouvoir de contrainte équivalent, pour leur permettre d'exécuter leur mission d'inspection.

9. Si, en vertu du droit national, l'assistance prévue au paragraphe 8 du présent article requiert l'autorisation d'une autorité judiciaire, la Commission, l'autorité nationale compétente de l'État membre chargée de faire appliquer les règles visées à l'article 1er, paragraphe 6, ou les agents mandatés par ces autorités la sollicitent. Cette autorisation peut également être sollicitée par mesure de précaution.

10. Lorsqu'une autorisation visée au paragraphe 9 du présent article est sollicitée, l'autorité judiciaire nationale vérifie que la décision de la Commission est authentique et que les mesures coercitives envisagées ne sont ni arbitraires ni excessives par rapport à l'objet de l'inspection. Lorsqu'elle contrôle la proportionnalité des mesures coercitives, l'autorité judiciaire nationale peut demander à la Commission, directement ou par l'intermédiaire de l'autorité nationale compétente de l'État membre chargée de faire appliquer les règles visées à l'article 1er, paragraphe 6, des explications détaillées, notamment sur les motifs qui incitent la Commission à suspecter une infraction au présent règlement, ainsi que sur la gravité de l'infraction suspectée et sur la nature de l'implication de l'entreprise concernée. Cependant,

l’autorité judiciaire nationale ne peut ni remettre en cause la nécessité de l’inspection ni exiger la communication des informations figurant dans le dossier de la Commission. Le contrôle de la légalité de la décision de la Commission est réservé à la Cour de justice.

Article 24

Mesures provisoires

En cas d’urgence justifiée par le fait qu’un préjudice grave et irréparable risque d’être causé aux entreprises utilisatrices ou aux utilisateurs finaux des contrôleurs d’accès, la Commission peut adopter un acte d’exécution ordonnant des mesures provisoires à l’encontre d’un contrôleur d’accès sur la base d’un constat prima facie d’infraction à l’article 5, 6 ou 7. Cet acte d’exécution est uniquement adopté dans le cadre d’une procédure ouverte en vue de l’adoption éventuelle d’une décision constatant un non-respect en application de l’article 29, paragraphe 1. Il est uniquement applicable pour une durée déterminée et est renouvelable dans la mesure où cela est nécessaire et opportun. Cet acte d’exécution est adopté en conformité avec la procédure consultative visée à l’article 50, paragraphe 2.

Article 25

Engagements

1. Si, au cours d’une procédure prévue par l’article 18, le contrôleur d’accès concerné propose de prendre des engagements pour les services de plateforme essentiels en cause afin de garantir le respect des obligations énoncées aux articles 5, 6 et 7, la Commission peut adopter un acte d’exécution rendant ces engagements obligatoires pour ce contrôleur d’accès et déclarer qu’il n’y a plus lieu d’agir. Cet acte d’exécution est adopté en conformité avec la procédure consultative visée à l’article 50, paragraphe 2.

2. La Commission peut, sur demande ou de sa propre initiative, rouvrir la procédure concernée par voie de décision lorsque:

a)

l’un des faits sur lesquels la décision repose subit un changement important;

b)

le contrôleur d’accès concerné contrevient à ses engagements;

c)

la décision repose sur des informations incomplètes, inexactes ou dénaturées fournies par les parties;

d)

les engagements ne sont pas effectifs.

3. Si la Commission devait estimer que les engagements proposés par le contrôleur d'accès concerné ne peuvent pas garantir le respect effectif des obligations prévues aux articles 5, 6 et 7, elle explique les raisons pour lesquelles elle ne rend pas ces engagements obligatoires dans la décision concluant la procédure en question.

Article 26

Contrôle des obligations et mesures

1. La Commission prend les mesures nécessaires pour contrôler la mise en œuvre et le respect effectifs des obligations prévues aux articles 5, 6 et 7 et des décisions prises en vertu des articles 8, 18, 24, 25 et 29. Ces mesures peuvent notamment consister à imposer au contrôleur d'accès l'obligation de conserver tous les documents jugés pertinents pour évaluer la mise en œuvre et le respect de ces obligations et décisions.

2. Les mesures visées au paragraphe 1 peuvent comprendre la nomination d'experts et d'auditeurs externes indépendants, ainsi que la désignation d'agents par les autorités nationales compétentes des États membres, pour aider la Commission à contrôler les obligations et mesures et lui apporter une expertise et des connaissances spécifiques.

Article 27

Renseignements en provenance de tiers

1. Tous les tiers, y compris les entreprises utilisatrices, les concurrents ou les utilisateurs finaux des services de plateforme essentiels énumérés dans la décision de désignation en vertu de l'article 3, paragraphe 9, ainsi que leurs représentants, peuvent informer l'autorité nationale compétente de l'État membre, chargée de faire appliquer les règles visées à l'article 1er, paragraphe 6, ou directement la Commission concernant toute pratique ou tout comportement des contrôleurs d'accès relevant du champ d'application du présent règlement.

2. L'autorité nationale compétente de l'État membre, chargée de faire appliquer les règles visées à l'article 1er, paragraphe 6, et la Commission ont toute latitude en ce qui concerne les mesures appropriées et ne sont pas tenues de donner suite aux renseignements reçus.

3. Lorsque l'autorité nationale compétente de l'État membre, chargée de faire appliquer les règles visées à l'article 1er, paragraphe 6, détermine, sur la base des renseignements reçus en vertu du paragraphe 1 du présent article, qu'il peut y avoir un cas de non-respect du présent règlement, elle transmet ces renseignements à la Commission.

Article 28

Fonction de vérification de la conformité

1. Les contrôleurs d'accès mettent en place une fonction de vérification de la conformité, qui est indépendante des fonctions opérationnelles du contrôleur d'accès et fait appel à un ou plusieurs responsables de la conformité, y compris le responsable général de la fonction de vérification de la conformité.

2. Le contrôleur d’accès veille à ce que la fonction de vérification de la conformité visée au paragraphe 1 dispose d’une autorité, d’une stature et de ressources suffisantes, ainsi que d’un accès à l’organe de direction du contrôleur d’accès pour contrôler le respect du présent règlement par ce dernier.

3. L’organe de direction du contrôleur d’accès s’assure que les responsables de la conformité désignés conformément au paragraphe 1 disposent des qualifications professionnelles, des connaissances, de l’expérience et des aptitudes nécessaires pour mener à bien les tâches visées au paragraphe 5.

L’organe de direction du contrôleur d’accès veille également à ce que le responsable général de la fonction de vérification de la conformité soit un cadre supérieur ayant une responsabilité distincte pour la fonction de vérification de la conformité.

4. Le responsable général de la fonction de vérification de la conformité fait directement rapport à l’organe de direction du contrôleur d’accès et peut soulever des préoccupations et avertir cet organe en cas de risque de non-respect du présent règlement, sans préjudice des responsabilités de l’organe de direction dans ses fonctions de surveillance et de gestion.

Il ne peut être congédié sans l’accord préalable de l’organe de direction du contrôleur d’accès.

5. Les responsables de la conformité désignés par le contrôleur d’accès en vertu du paragraphe 1 sont chargés des tâches suivantes:

a)

organiser, suivre et contrôler les mesures et activités des contrôleurs d’accès visant à assurer le respect du présent règlement;

b)

informer et conseiller la direction et les employés du contrôleur d’accès en ce qui concerne le respect du présent règlement;

c)

contrôler, le cas échéant, le respect des engagements rendus contraignants en vertu de l’article 25, sans préjudice de la possibilité pour la Commission de désigner des experts externes indépendants conformément à l’article 26, paragraphe 2;

d)

coopérer avec la Commission aux fins du présent règlement.

6. Les contrôleurs d’accès communiquent à la Commission le nom et les coordonnées du responsable général de la fonction de vérification de la conformité.

7. L’organe de direction du contrôleur d’accès définit, supervise et rend compte de la mise en œuvre des dispositifs de gouvernance du contrôleur d’accès qui garantissent l’indépendance de la fonction de vérification de la conformité, y compris la répartition des

responsabilités dans l'organisation du contrôleur d'accès et la prévention des conflits d'intérêts.

8. L'organe de direction approuve et réexamine périodiquement, au moins une fois par an, les stratégies et les politiques relatives à la prise en compte, à la gestion et au suivi du respect du présent règlement.

9. L'organe de direction consacre suffisamment de temps à la gestion et au suivi du respect du présent règlement. Il participe activement aux décisions relatives à la gestion et à l'exécution du présent règlement et veille à ce que des ressources suffisantes soient allouées en la matière.

Article 29

Non-respect

1. La Commission adopte un acte d'exécution établissant son constat de non-respect (ci-après dénommé «décision constatant un non-respect») lorsqu'elle constate qu'un contrôleur d'accès ne respecte pas un ou plusieurs des éléments suivants:

a)

l'une des obligations prévues à l'article 5, 6 ou 7;

b)

les mesures précisées par la Commission dans une décision adoptée en vertu de l'article 8, paragraphe 2;

c)

les mesures correctives imposées en vertu de l'article 18, paragraphe 1;

d)

les mesures provisoires ordonnées en vertu de l'article 24; ou

e)

les engagements rendus juridiquement obligatoires en vertu de l'article 25.

Cet acte d'exécution est adopté en conformité avec la procédure consultative visée à l'article 50, paragraphe 2.

2. La Commission s'efforce d'adopter sa décision constatant un non-respect dans les douze mois suivant l'ouverture de la procédure prévue à l'article 20.

3. Avant d'adopter la décision constatant un non-respect, la Commission fait part de ses constatations préliminaires au contrôleur d'accès concerné. Dans ces constatations préliminaires, la Commission explique les mesures qu'elle envisage de prendre ou que le

contrôleur d’accès devrait prendre, selon elle, afin de donner suite de manière effective aux constatations préliminaires.

4. Lorsqu’elle prévoit d’adopter une décision constatant un non-respect, la Commission peut consulter des tiers.

5. Dans la décision constatant un non-respect, la Commission ordonne au contrôleur d’accès de mettre fin au non-respect dans un délai approprié et de fournir des explications sur la manière dont il envisage de se mettre en conformité avec cette décision.

6. Le contrôleur d’accès fournit à la Commission la description des mesures qu’il a prises pour garantir le respect de la décision constatant un non-respect.

7. Lorsque la Commission décide de ne pas adopter une décision constatant un non-respect, elle clôt la procédure par voie de décision.

Article 30

Amendes

1. Dans la décision constatant un non-respect, la Commission peut infliger à un contrôleur d’accès des amendes jusqu’à concurrence de 10 % de son chiffre d’affaires total réalisé au niveau mondial au cours de l’exercice précédent lorsqu’elle constate que le contrôleur d’accès, volontairement ou par négligence, ne respecte pas:

a)

l’une des obligations prévues aux articles 5, 6 et 7;

b)

les mesures précisées par la Commission dans une décision adoptée en vertu de l’article 8, paragraphe 2;

c)

les mesures correctives imposées en vertu de l’article 18, paragraphe 1;

d)

les mesures provisoires ordonnées en vertu de l’article 24; ou

e)

les engagements rendus juridiquement obligatoires en vertu de l’article 25.

2. Nonobstant le paragraphe 1 du présent article, dans une décision constatant un non-respect, la Commission peut infliger à un contrôleur d’accès des amendes allant jusqu’à 20 % de son chiffre d’affaires total réalisé au niveau mondial au cours de l’exercice précédent lorsqu’elle constate qu’un contrôleur d’accès a commis la même infraction à une obligation

prévue à l'article 5, 6 ou 7, ou une infraction similaire, en ce qui concerne le même service de plateforme essentiel que celui pour lequel une infraction avait été constatée dans une décision constatant un non-respect adoptée au cours des huit années précédentes.

3. La Commission peut adopter une décision infligeant aux entreprises, y compris aux contrôleurs d'accès le cas échéant, et aux associations d'entreprises, des amendes jusqu'à concurrence de 1 % de leur chiffre d'affaires total réalisé au niveau mondial au cours de l'exercice précédent lorsque, volontairement ou par négligence, elles:

a)

ne fournissent pas, dans le délai imparti, les renseignements requis pour l'appréciation de leur désignation comme contrôleurs d'accès en vertu de l'article 3 ou fournissent des renseignements inexacts, incomplets ou dénaturés;

b)

ne respectent pas l'obligation d'information de la Commission prévue à l'article 3, paragraphe 3;

c)

ne communiquent pas les renseignements exigés conformément à l'article 14, ou fournissent des renseignements inexacts, incomplets ou dénaturés;

d)

ne présentent pas la description exigée au titre de l'article 15 ou fournissent des renseignements inexacts, incomplets ou dénaturés;

e)

ne donnent pas l'accès aux données et algorithmes ou aux renseignements concernant les essais en réponse à une demande faite en vertu de l'article 21, paragraphe 3;

f)

ne fournissent pas les renseignements exigés dans le délai fixé en vertu de l'article 21, paragraphe 3, ou fournissent des renseignements ou des explications, qui sont exigés en vertu de l'article 21 ou fournis lors d'une audition en vertu de l'article 22, inexacts, incomplets ou dénaturés;

g)

omettent de rectifier, dans le délai fixé par la Commission, les renseignements inexacts, incomplets ou dénaturés donnés par un représentant ou un membre du personnel, ou omettent ou refusent de fournir des renseignements complets sur des faits en rapport avec l'objet et le but d'une inspection décidée en vertu de l'article 23;

h)

refusent de se soumettre à une inspection décidée en vertu de l'article 23;

i)

ne se conforment pas aux obligations imposées par la Commission en vertu de l'article 26; ou

j)

n'introduisent pas une fonction de vérification de la conformité conformément à l'article 28; ou

k)

ne respectent pas les conditions d'accès au dossier de la Commission conformément à l'article 34, paragraphe 4.

4. Pour déterminer le montant d'une amende, la Commission tient compte de la gravité, de la durée et de la récurrence ainsi que, pour les amendes infligées au titre du paragraphe 3, du retard causé à la procédure.

5. Lorsqu'une amende est infligée à une association d'entreprises en tenant compte du chiffre d'affaires de ses membres réalisé au niveau mondial et que cette association n'est pas solvable, cette dernière est tenue de lancer à ses membres un appel à contributions pour couvrir le montant de l'amende.

Si ces contributions n'ont pas été versées à l'association d'entreprises dans un délai fixé par la Commission, celle-ci peut exiger le paiement de l'amende directement par toute entreprise dont les représentants étaient membres des organes décisionnels concernés de ladite association.

Après avoir exigé le paiement conformément au deuxième alinéa, la Commission peut, lorsque cela est nécessaire pour garantir le paiement intégral de l'amende, exiger le paiement du solde par l'un quelconque des membres de l'association d'entreprises.

Cependant, la Commission n'exige pas le paiement visé au deuxième ou au troisième alinéa auprès des entreprises qui démontrent qu'elles n'ont pas appliqué la décision de l'association d'entreprises qui enfreignait le présent règlement et que soit elles en ignoraient l'existence, soit elles s'en étaient activement désolidarisées avant que la Commission n'ouvre une procédure en vertu de l'article 20.

La responsabilité financière de chaque entreprise en ce qui concerne le paiement de l'amende ne peut excéder 20 % de son chiffre d'affaires total réalisé au niveau mondial au cours de l'exercice précédent.

Article 31

Astreintes

1. La Commission peut adopter une décision infligeant aux entreprises, y compris aux contrôleurs d'accès s'il y a lieu, et aux associations d'entreprises des astreintes jusqu'à concurrence de 5 % du chiffre d'affaires journalier moyen réalisé au niveau mondial au cours de l'exercice précédent par jour, à compter de la date qu'elle fixe dans sa décision, pour les contraindre:

a)

à respecter les mesures précisées par la Commission dans une décision adoptée en vertu de l'article 8, paragraphe 2;

b)

à respecter la décision prise en vertu de l'article 18, paragraphe 1;

c)

à fournir des renseignements exacts et complets dans le délai requis par une demande de renseignements formulée par voie de décision en vertu de l'article 21;

d)

à garantir l'accès aux données, algorithmes et renseignements concernant les essais en réponse à une demande faite en vertu de l'article 21, paragraphe 3, et à fournir des explications les concernant, tel qu'exigé par une décision prise en vertu de l'article 21;

e)

à se soumettre à une inspection ordonnée par voie de décision prise en vertu de l'article 23;

f)

à respecter une décision ordonnant des mesures provisoires prises en vertu de l'article 24;

g)

à respecter des engagements rendus juridiquement obligatoires par décision en vertu de l'article 25, paragraphe 1;

h)

à respecter une décision prise en application de l'article 29, paragraphe 1.

2. Lorsque les entreprises, ou associations d'entreprises, ont satisfait à l'obligation pour l'exécution de laquelle l'astreinte a été infligée, la Commission peut adopter un acte d'exécution fixant le montant définitif de l'astreinte à un chiffre inférieur à celui qui résulte de la décision initiale. Cet acte d'exécution est adopté en conformité avec la procédure consultative visée à l'article 50, paragraphe 2.

Article 32

Prescription en matière d’imposition de sanctions

1. Les pouvoirs conférés à la Commission en vertu des articles 30 et 31 sont soumis à un délai de prescription de cinq ans.

2. La prescription court à compter du jour où l’infraction a été commise. Toutefois, pour les infractions continues ou répétées, la prescription ne court qu’à compter du jour où l’infraction a pris fin.

3. La prescription en matière d’imposition d’amendes ou d’astreintes est interrompue par tout acte de la Commission visant à mener une enquête sur le marché ou à poursuivre l’infraction. L’interruption de la prescription prend effet le jour où l’acte est notifié à au moins une entreprise ou association d’entreprises ayant participé à l’infraction. Constituent notamment des actes interrompant la prescription:

a)

les demandes de renseignements de la Commission;

b)

les autorisations écrites d’effectuer des inspections délivrées par la Commission à ses agents;

c)

l’ouverture d’une procédure par la Commission en application de l’article 20.

4. La prescription court à nouveau à partir de chaque interruption. Toutefois, la prescription est acquise au plus tard le jour où un délai égal au double du délai de prescription arrive à expiration sans que la Commission ait prononcé une amende ou astreinte. Ce délai est prolongé de la période pendant laquelle la prescription est suspendue conformément au paragraphe 5.

5. La prescription en matière d’imposition d’amendes ou d’astreintes est suspendue aussi longtemps que la décision de la Commission fait l’objet d’une procédure pendante devant la Cour de justice.

Article 33

Prescription en matière d’exécution des sanctions

1. Le pouvoir de la Commission d’exécuter les décisions prises en vertu des articles 30 et 31 est soumis à un délai de prescription de cinq ans.

2. La prescription court à compter du jour où la décision est devenue définitive.

3. La prescription en matière d’exécution des sanctions est interrompue:

a)

par la notification d’une décision modifiant le montant initial de l’amende ou de l’astreinte ou rejetant une demande tendant à obtenir une telle modification; ou

b)

par tout acte de la Commission ou d’un État membre, agissant à la demande de la Commission, visant au recouvrement forcé de l’amende ou de l’astreinte.

4. La prescription court à nouveau à partir de chaque interruption.

5. La prescription en matière d’exécution des sanctions est suspendue:

a)

aussi longtemps qu’un délai de paiement est accordé; ou

b)

aussi longtemps que l’exécution forcée du paiement est suspendue en vertu d’une décision de la Cour de justice ou d’une décision d’une juridiction nationale.

Article 34

Droit d’être entendu et droit d’accès au dossier

1. Avant d’adopter une décision au titre de l’article 8, de l’article 9, paragraphe 1, de l’article 10, paragraphe 1, des articles 17, 18, 24, 25, 29 et 30 et de l’article 31, paragraphe 2, la Commission donne au contrôleur d’accès ou à l’entreprise ou à l’association d’entreprises concerné l’occasion de faire connaître son point de vue sur:

a)

les constatations préliminaires de la Commission, y compris sur tout grief retenu par la Commission; et

b)

les mesures que la Commission peut avoir l’intention de prendre au vu des constatations préliminaires visées au point a) du présent paragraphe.

2. Les contrôleurs d’accès, les entreprises et les associations d’entreprises concernés peuvent présenter à la Commission leurs observations en ce qui concerne les constatations préliminaires de la Commission dans un délai fixé par la Commission dans ses constatations préliminaires et qui ne peut être inférieur à 14 jours.

3. La Commission ne fonde ses décisions que sur les constatations préliminaires, y compris sur tout grief retenu par la Commission, au sujet desquelles les contrôleurs d’accès, les entreprises et les associations d’entreprises concernés ont pu faire valoir leurs observations.

4. Les droits de la défense du contrôleur d'accès, de l'entreprise ou de l'association d'entreprises concerné sont pleinement assurés dans le déroulement de la procédure. Le contrôleur d'accès, l'entreprise ou l'association d'entreprises concerné a le droit d'avoir accès au dossier de la Commission conformément aux modalités de divulgation, sous réserve de l'intérêt légitime des entreprises à ce que leurs secrets d'affaires ne soient pas divulgués. En cas de désaccord entre les parties, la Commission peut adopter des décisions fixant ces modalités de divulgation. Le droit d'accès au dossier de la Commission ne s'étend pas aux informations confidentielles et aux documents internes de la Commission ou des autorités compétentes des États membres. En particulier, le droit d'accès ne s'étend pas à la correspondance entre la Commission et les autorités compétentes des États membres. Aucune disposition du présent paragraphe n'empêche la Commission de divulguer et d'utiliser des informations nécessaires pour apporter la preuve d'une infraction.

Article 35

Rapports annuels

1. La Commission présente au Parlement européen et au Conseil un rapport annuel sur la mise en œuvre du présent règlement et sur les progrès accomplis dans la réalisation de ses objectifs.

2. Le rapport visé au paragraphe 1 comprend:

a)

un résumé des activités de la Commission, y compris toute mesure ou décision adoptée et les enquêtes de marché en cours en rapport avec le présent règlement;

b)

les constatations résultant du suivi de la mise en œuvre par les contrôleurs d'accès des obligations au titre du présent règlement;

c)

une évaluation de la description ayant fait l'objet d'un audit visée à l'article 15;

d)

une vue d'ensemble de la coopération entre la Commission et les autorités nationales dans le cadre du présent règlement;

e)

un aperçu des activités et des tâches effectuées par le groupe de haut niveau des régulateurs numériques, y compris la manière dont ses recommandations concernant l'application du présent règlement doivent être mises en œuvre.

3. La Commission publie le rapport sur son site internet.

Article 36

Secret professionnel

1. Les informations recueillies en vertu du présent règlement sont utilisées aux fins de celui-ci.

2. Les informations recueillies en vertu de l'article 14 sont utilisées aux fins du présent règlement, du règlement (CE) no 139/2004 et des règles nationales en matière de concentration.

3. Les informations recueillies en vertu de l'article 15 sont utilisées aux fins du présent règlement et du règlement (UE) 2016/679.

4. Sans préjudice de l'échange et de l'utilisation des informations fournies aux fins d'utilisation selon les articles 38, 39, 41 et 43, la Commission, les autorités compétentes des États membres, leurs fonctionnaires, agents et les autres personnes travaillant sous la supervision de ces autorités, ainsi que toute personne physique ou morale, dont les auditeurs et experts nommés en vertu de l'article 26, paragraphe 2, sont tenus de ne pas divulguer les informations qu'ils ont recueillies ou échangées en application du présent règlement et qui, par leur nature, sont couvertes par le secret professionnel.

Article 37

Coopération avec les autorités nationales

1. La Commission et les États membres travaillent en étroite coopération et coordonnent leurs mesures d'exécution pour assurer une application cohérente, efficace et complémentaire des instruments juridiques disponibles appliqués aux contrôleurs d'accès au sens du présent règlement.

2. La Commission peut, le cas échéant, consulter les autorités nationales sur toute question relative à l'application du présent règlement.

Article 38

Coopération et coordination avec les autorités nationales compétentes chargées de faire appliquer les règles de concurrence

1. La Commission et les autorités nationales compétentes des États membres chargées de faire appliquer les règles visées à l'article 1er, paragraphe 6, coopèrent les unes avec les autres et s'échangent des informations sur leurs mesures d'exécution respectives par l'intermédiaire du Réseau européen de la concurrence (REC). Elles ont le pouvoir de se communiquer toute information relative à un élément de fait ou de droit, y compris s'il s'agit d'une information confidentielle. Si l'autorité compétente n'est pas membre du REC, la Commission établit les modalités nécessaires pour cette coopération et cet échange d'informations sur les dossiers concernant l'application du présent règlement et l'application des règles dans les cas visés à l'article 1er, paragraphe 6. La Commission peut établir ces modalités dans un acte d'exécution visé à l'article 46, paragraphe 1, point l).

2. Lorsqu'une autorité nationale compétente d'un État membre chargée de faire appliquer les règles visées à l'article 1er, paragraphe 6, a l'intention d'ouvrir une enquête sur des contrôleurs d'accès en application de dispositions législatives nationales visées à l'article 1er, paragraphe 6, elle informe la Commission par écrit de la première mesure d'enquête formelle, avant ou immédiatement après le début de cette mesure. Cette information peut également être mise à la disposition des autorités nationales compétentes chargées de faire appliquer les règles visées à l'article 1er, paragraphe 6, des autres États membres.

3. Lorsqu'une autorité nationale compétente d'un État membre chargée de faire appliquer les règles visées à l'article 1er, paragraphe 6, a l'intention d'imposer des obligations à des contrôleurs d'accès en application de dispositions législatives nationales visées à l'article 1er, paragraphe 6, elle communique le projet de mesure et ses motifs à la Commission, au plus tard 30 jours avant son adoption. Dans le cas de mesures provisoires, l'autorité nationale compétente d'un État membre chargée de faire appliquer les règles visées à l'article 1er, paragraphe 6, communique à la Commission les projets de mesures envisagées dès que possible et au plus tard immédiatement après l'adoption de ces mesures. Cette information peut également être mise à la disposition des autorités nationales compétentes chargées de faire appliquer les règles visées à l'article 1er, paragraphe 6, des autres États membres.

4. Les mécanismes d'information prévus aux paragraphes 2 et 3 ne s'appliquent pas aux décisions envisagées en vertu des règles nationales en matière de concentrations.

5. Les informations échangées en vertu des paragraphes 1 à 3 du présent article ne sont échangées et utilisées qu'aux fins de la coordination de l'application du présent règlement et des règles visées à l'article 1er, paragraphe 6.

6. La Commission peut demander aux autorités nationales compétentes des États membres chargées de faire appliquer les règles visées à l'article 1er, paragraphe 6, de soutenir toute enquête de marché qu'elle mène en application du présent règlement.

7. Lorsque, en vertu du droit national, une autorité nationale compétente d'un État membre chargée de faire appliquer les règles visées à l'article 1er, paragraphe 6, dispose de la compétence et des pouvoirs d'enquête voulus, elle peut, de sa propre initiative, mener une enquête sur un cas de non-respect éventuel des articles 5, 6 et 7 du présent règlement sur son territoire. Avant de prendre une première mesure d'enquête formelle, cette autorité en informe la Commission par écrit.

L'ouverture d'une procédure par la Commission en vertu de l'article 20 enlève aux autorités nationales compétentes des États membres chargées de contrôler le respect des règles visées à l'article 1er, paragraphe 6, la possibilité de mener une telle enquête ou de la clôturer lorsqu'elle est déjà en cours. Ces autorités communiquent à la Commission les résultats de l'enquête en question afin d'appuyer la Commission dans son rôle de seule instance habilitée à faire appliquer le présent règlement.

Article 39

Coopération avec les juridictions nationales

1. Dans le cadre des procédures engagées pour l'application du présent règlement, les juridictions nationales peuvent demander à la Commission de leur transmettre des

informations en sa possession ou son avis sur des questions relatives à l'application du présent règlement.

2. Les États membres transmettent à la Commission une copie de toute décision écrite des juridictions nationales statuant sur l'application du présent règlement. Cette copie est transmise sans tarder lorsque le jugement complet est notifié par écrit aux parties.

3. Lorsqu'une application cohérente du présent règlement l'exige, la Commission, agissant de sa propre initiative, peut présenter des observations écrites aux juridictions nationales. Avec l'autorisation de la juridiction concernée, elle peut aussi présenter des observations orales.

4. Aux seules fins de l'élaboration de ses observations, la Commission peut demander à la juridiction nationale concernée de lui transmettre ou de lui faire transmettre tout document nécessaire à l'appréciation de l'affaire.

5. Les juridictions nationales ne prennent aucune décision qui va à l'encontre d'une décision adoptée par la Commission en vertu du présent règlement. Elles évitent également de prendre des décisions qui iraient à l'encontre d'une décision envisagée par la Commission dans une procédure qu'elle a intentée en vertu du présent règlement. À cette fin, la juridiction nationale peut évaluer s'il est nécessaire de suspendre sa procédure. Cette disposition est sans préjudice de la possibilité qu'ont les juridictions nationales d'introduire une demande de décision préjudicielle conformément à l'article 267 du traité sur le fonctionnement de l'Union européenne.

Article 40

Le groupe de haut niveau

1. La Commission met en place un groupe de haut niveau pour le règlement sur les marchés numériques (ci-après dénommé «groupe de haut niveau»).

2. Le groupe de haut niveau se compose des organes et réseaux européens suivants:

a)

l'organe des régulateurs européens des communications électroniques,

b)

le Contrôleur européen de la protection des données et le comité européen de la protection des données,

c)

le réseau européen de la concurrence,

d)

le réseau de coopération en matière de protection des consommateurs, et

e)

le groupe des régulateurs européens pour les services de médias audiovisuels.

3. Les organes et réseaux européens visés au paragraphe 2 ont chacun un nombre égal de représentants au sein du groupe de haut niveau. Le nombre maximal de membres du groupe de haut niveau ne dépasse pas trente personnes.

4. La Commission fournit des services de secrétariat au groupe de haut niveau afin de faciliter ses travaux. Le groupe de haut niveau est présidé par la Commission, qui participe à ses réunions. Le groupe de haut niveau se réunit à la demande de la Commission au moins une fois par année civile. La Commission convoque également une réunion du groupe à la demande de la majorité des membres qui le composent afin de traiter une question spécifique.

5. Le groupe de haut niveau peut fournir à la Commission des conseils et une expertise dans les domaines relevant de la compétence de ses membres, notamment:

a)

des conseils et des recommandations relevant de leur expertise et présentant un intérêt pour toute question générale quant à la mise en œuvre ou à l'application du présent règlement; ou

b)

des conseils et une expertise en faveur d'une approche réglementaire cohérente entre les différents instruments réglementaires.

6. Le groupe de haut niveau peut, en particulier, recenser et évaluer les interactions actuelles et potentielles entre le présent règlement et les règles sectorielles appliquées par les autorités nationales composant les organismes et réseaux européens visés au paragraphe 2 et soumettre à la Commission un rapport annuel présentant cette évaluation et recensant les éventuels problèmes transréglementaires. Ce rapport peut être accompagné de recommandations visant à converger vers des approches transdisciplinaires cohérentes et des synergies entre la mise en œuvre du présent règlement et celle d'autres réglementations sectorielles. Ce rapport est communiqué au Parlement européen et au Conseil.

7. Dans le cadre d'enquêtes de marché sur de nouveaux services et de nouvelles pratiques, le groupe de haut niveau peut apporter son expertise à la Commission sur la nécessité de modifier, d'ajouter ou de supprimer des règles figurant dans le présent règlement afin de faire en sorte que les marchés numériques dans l'ensemble de l'Union soient contestables et équitables.

Article 41

Demande d'enquête de marché

1. Trois États membres ou plus peuvent solliciter auprès de la Commission l'ouverture d'une enquête de marché conformément à l'article 17 parce qu'il existe, selon eux, des motifs

raisonnables de soupçonner qu'une entreprise devrait être désignée comme contrôleur d'accès.

2. Un ou plusieurs États membres peuvent demander à la Commission d'ouvrir une enquête de marché conformément à l'article 18 parce qu'il existe, selon eux, des motifs raisonnables de soupçonner qu'un contrôleur d'accès a systématiquement contrevenu à une ou plusieurs des obligations prévues aux articles 5, 6 et 7, et qu'il a maintenu, renforcé ou étendu sa position de contrôleur d'accès au regard des caractéristiques énoncées à l'article 3, paragraphe 1.

3. Trois États membres ou plus peuvent solliciter auprès de la Commission l'ouverture d'une enquête de marché conformément à l'article 19 parce qu'il existe, selon eux, des motifs raisonnables de soupçonner:

a)

qu'il faudrait ajouter davantage de services relevant du secteur numérique à la liste des services de plateforme essentiels établie à l'article 2, point 2); ou

b)

que le présent règlement ne permet pas de remédier de manière effective à une ou plusieurs pratiques et que ces pratiques sont susceptibles de limiter la contestabilité des service de plateforme essentiels ou d'être inéquitables.

4. Les États membres apportent des éléments de preuve à l'appui de leurs demandes introduites en vertu des paragraphes 1, 2 et 3. Pour les demandes introduites en vertu du paragraphe 3, ces éléments de preuve peuvent inclure des informations sur les offres nouvelles de produits, de services, de logiciels ou de fonctionnalités qui suscitent des préoccupations du point de vue de la contestabilité ou de l'équité, qu'elles soient mises en œuvre dans le cadre de services de plateforme essentiels existants ou d'une autre façon.

5. Dans les quatre mois suivant la réception d'une demande introduite en vertu du présent article, la Commission examine s'il existe des motifs raisonnables pour ouvrir une enquête de marché en vertu du paragraphe 1, 2 ou 3. La Commission publie les résultats de cette évaluation.

Article 42

Actions représentatives

La directive (UE) 2020/1828 est applicable aux actions représentatives intentées en raison des infractions commises par des contrôleurs d'accès aux dispositions du présent règlement qui portent atteinte ou risquent de porter atteinte aux intérêts collectifs des consommateurs.

Article 43

Signalement de violations et protection des auteurs de signalement

Le signalement de toutes les violations du présent règlement et la protection des personnes signalant ces violations sont régis par la directive (UE) 2019/1937.

CHAPITRE VI

DISPOSITIONS FINALES

Article 44

Publication des décisions

1. La Commission publie les décisions qu'elle prend au titre des articles 3 et 4, de l'article 8, paragraphe 2, des articles 9, 10, 16 à 20 et 24, de l'article 25, paragraphe 1, et des articles 29, 30 et 31. Cette publication mentionne le nom des parties intéressées et l'essentiel de la décision, y compris les sanctions imposées.

2. La publication tient compte de l'intérêt légitime des contrôleurs d'accès ou des tiers à ce que leurs informations confidentielles ne soient pas divulguées.

Article 45

Contrôle de la Cour de justice

Conformément à l'article 261 du traité sur le fonctionnement de l'Union européenne, la Cour de justice statue avec compétence de pleine juridiction sur les recours dirigés contre les décisions par lesquelles la Commission inflige des amendes ou des astreintes. Elle peut supprimer, réduire ou majorer l'amende ou l'astreinte infligée.

Article 46

Dispositions d'exécution

1. La Commission peut adopter des actes d'exécution établissant les modalités détaillées pour l'application de ce qui suit:

a)

la forme, la teneur et les autres modalités des notifications et mémoires présentés en application de l'article 3;

b)

la forme, la teneur et les autres modalités des mesures techniques que les contrôleurs d'accès mettent en œuvre pour garantir le respect de l'article 5, 6 ou 7;

c)

les modalités opérationnelles et techniques en vue de la mise en œuvre de l'interopérabilité des services de communications interpersonnelles non fondés sur la numérotation conformément à l'article 7;

d)

la forme, la teneur et les autres modalités de la demande motivée présentée en application de l'article 8, paragraphe 3;

e)

la forme, la teneur et les autres modalités des demandes motivées présentées en application des articles 9 et 10;

f)

la forme, la teneur et les autres modalités des rapports réglementaires communiqués en application de l'article 11;

g)

la méthodologie et la procédure pour la description, devant faire l'objet d'un audit, des techniques utilisées pour le profilage des consommateurs prévue à l'article 15, paragraphe 1; lorsqu'elle élabore un projet d'acte d'exécution à cette fin, la Commission consulte le Contrôleur européen de la protection des données et peut consulter le comité européen de la protection des données, la société civile et d'autres experts compétents;

h)

la forme, la teneur et les autres modalités des notifications et mémoires présentés en application des articles 14 et 15;

i)

les modalités des procédures relatives aux enquêtes de marché prévues aux articles 17, 18 et 19 et des procédures définies aux articles 24, 25 et 29;

j)

les modalités d'exercice du droit d'être entendu prévu à l'article 34;

k)

les modalités pour les conditions de la divulgation prévue à l'article 34;

l)

les modalités de la coopération et de la coordination entre la Commission et les autorités nationales prévues aux articles 37 et 38; et

m)

les modalités de calcul et de prolongation des délais.

2. Les actes d'exécution visés au paragraphe 1, points a) à k) et m), du présent article sont adoptés en conformité avec la procédure consultative visée à l'article 50, paragraphe 2.

L'acte d'exécution visé au paragraphe 1, point l), du présent article est adopté en conformité avec la procédure d'examen visée à l'article 50, paragraphe 3.

3. Avant l'adoption de tout acte d'exécution en vertu du paragraphe 1, la Commission en publie le projet et invite toutes les parties intéressées à lui soumettre leurs observations dans un délai qui ne peut être inférieur à un mois.

Article 47

Lignes directrices

La Commission peut adopter des lignes directrices sur tout aspect du présent règlement afin de faciliter sa mise en œuvre et son application effectives.

Article 48

Normalisation

Si elle le juge opportun et nécessaire, la Commission peut charger les organisations européennes de normalisation d'élaborer des normes appropriées pour faciliter la mise en œuvre des obligations fixées dans le présent règlement.

Article 49

Exercice de la délégation

1. Le pouvoir d'adopter des actes délégués conféré à la Commission est soumis aux conditions fixées au présent article.

2. Le pouvoir d'adopter des actes délégués visé à l'article 3, paragraphes 6 et 7, et à l'article 12, paragraphes 1, 3 et 4, est conféré à la Commission pour une période de cinq ans à compter du 1er novembre 2022. La Commission élabore un rapport relatif à la délégation de pouvoir au plus tard neuf mois avant la fin de la période de cinq ans. La délégation de pouvoir est tacitement prorogée pour des périodes d'une durée identique, sauf si le Parlement européen ou le Conseil s'oppose à cette prorogation trois mois au plus tard avant la fin de chaque période.

3. La délégation de pouvoir visée à l'article 3, paragraphes 6 et 7, et à l'article 12, paragraphes 1, 3 et 4, peut être révoquée à tout moment par le Parlement européen ou le Conseil. La décision de révocation met fin à la délégation de pouvoir qui y est précisée. La révocation prend effet le jour suivant celui de la publication de ladite décision au Journal officiel de l'Union européenne ou à une date ultérieure qui est précisée dans ladite décision. Elle ne porte pas atteinte à la validité des actes délégués déjà en vigueur.

4. Avant l'adoption d'un acte délégué, la Commission consulte les experts désignés par chaque État membre, conformément aux principes définis dans l'accord interinstitutionnel du 13 avril 2016«Mieux légiférer».

5. Aussitôt qu'elle adopte un acte délégué, la Commission le notifie au Parlement européen et au Conseil simultanément.

6. Un acte délégué adopté en vertu de l'article 3, paragraphes 6 et 7, et de l'article 12, paragraphes 1, 3 et 4, n'entre en vigueur que si le Parlement européen ou le Conseil n'a pas exprimé d'objections dans un délai de deux mois à compter de la notification de cet acte au Parlement européen et au Conseil ou si, avant l'expiration de ce délai, le Parlement européen et le Conseil ont tous deux informé la Commission de leur intention de ne pas exprimer d'objections. Ce délai est prolongé de deux mois à l'initiative du Parlement européen ou du Conseil.

Article 50

Comité

1. La Commission est assistée par un comité (ci-après dénommé «comité consultatif en matière de marchés numériques»). Ledit comité est un comité au sens du règlement (UE) no 182/2011.

2. Lorsqu'il est fait référence au présent paragraphe, l'article 4 du règlement (UE) no 182/2011 s'applique.

Lorsque l'avis du comité doit être obtenu par procédure écrite, ladite procédure est close sans résultat lorsque, dans le délai pour émettre un avis, le président du comité le décide ou une majorité simple des membres du comité le demandent.

3. Lorsqu'il est fait référence au présent paragraphe, l'article 5 du règlement (UE) no 182/2011 s'applique.

4. La Commission fait part au destinataire d'une décision individuelle de l'avis du comité, accompagné de cette décision. Elle rend publics l'avis et la décision individuelle, en tenant compte de l'intérêt légitime à la protection du secret professionnel.

Article 51

Modification de la directive (UE) 2019/1937

À la partie I, point J, de l'annexe de la directive (UE) 2019/1937, le point suivant est ajouté:

«iv)

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 (règlement sur les marchés numériques) (JO L 265 du 21.9.2022, p. 1).».

Article 52

Modification de la directive (UE) 2020/1828

À l’annexe I de la directive (UE) 2020/1828, le point suivant est ajouté:

«67)

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 (règlement sur les marchés numériques) (JO L 265 du 21.9.2022, p. 1).».

Article 53

Réexamen

1. Au plus tard le 3 mai 2026, et tous les trois ans par la suite, la Commission évalue le présent règlement et fait rapport au Parlement européen, au Conseil et au Comité économique et social.

2. Les évaluations déterminent si les objectifs du présent règlement consistant à garantir que les marchés soient contestables et équitables ont été atteints, et elles mesurent l’incidence du présent règlement pour les entreprises utilisatrices, notamment les PME, et les utilisateurs finaux. De plus, la Commission évalue si le champ de l’article 7 peut être élargi aux services de réseaux sociaux en ligne.

3. Les évaluations déterminent s’il est nécessaire de modifier les règles, notamment en ce qui concerne la liste des services de plateforme essentiels établie à l’article 2, point 2), les obligations prévues aux articles 5, 6 et 7 et le contrôle de leur respect, afin de garantir la contestabilité et l’équité des marchés numériques dans l’Union. À la suite des évaluations, la Commission prend les mesures appropriées, qui peuvent comprendre des propositions législatives.

4. Les autorités compétentes des États membres communiquent toutes les informations pertinentes dont elles disposent que la Commission pourrait solliciter aux fins de l’établissement du rapport visé au paragraphe 1.

Article 54

Entrée en vigueur et application

Le présent règlement entre en vigueur le vingtième jour suivant celui de sa publication au Journal officiel de l’Union européenne.

Il est applicable à partir du 2 mai 2023.

Cependant, l’article 3, paragraphes 6 et 7, ainsi que les articles 40, 46, 47, 48, 49 et 50 sont applicables à partir du 1er novembre 2022, et les articles 42 et 43 sont applicables à partir du 25 juin 2023.

Toutefois, si la date du 25 juin 2023 précède la date d'application visée au deuxième alinéa du présent article, l'application des articles 42 et 43 est repoussée à la date d'application visée au deuxième alinéa du présent article.

Le présent règlement est obligatoire dans tous ses éléments et directement applicable dans tout État membre.

Fait à Strasbourg, le 14 septembre 2022

Par le Parlement européen

La présidente

R. METSOLA

Par le Conseil

Le président

M. BEK

(1) JO C 286 du 16.7.2021, p. 64.

(2) JO C 440 du 29.10.2021, p. 67.

(3) Position du Parlement européen du 5 juillet 2022 (non encore parue au Journal officiel) et décision du Conseil du 18 juillet 2022.

(4) 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) (JO L 119 du 4.5.2016, p. 1).

(5) Règlement (UE) 2019/1150 du Parlement européen et du Conseil du 20 juin 2019 promouvant l'équité et la transparence pour les entreprises utilisatrices de services d'intermédiation en ligne (JO L 186 du 11.7.2019, p. 57).

(6) Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques) (JO L 201 du 31.7.2002, p. 37).

(7) Directive 2005/29/CE du Parlement européen et du Conseil du 11 mai 2005 relative aux pratiques commerciales déloyales des entreprises vis-à-vis des consommateurs dans le marché intérieur et modifiant la directive 84/450/CEE du Conseil et les directives 97/7/CE, 98/27/CE et 2002/65/CE du Parlement européen et du Conseil et le règlement (CE) no 2006/2004 du Parlement européen et du Conseil («directive sur les pratiques commerciales déloyales») (JO L 149 du 11.6.2005, p. 22).

(8) Directive 2010/13/UE du Parlement européen et du Conseil du 10 mars 2010 visant à la coordination de certaines dispositions législatives, réglementaires et administratives des États membres relatives à la fourniture de services de médias audiovisuels (directive «Services de médias audiovisuels») (JO L 95 du 15.4.2010, p. 1).

(9) Directive (UE) 2015/2366 du Parlement européen et du Conseil du 25 novembre 2015 concernant les services de paiement dans le marché intérieur, modifiant les directives 2002/65/CE, 2009/110/CE et 2013/36/UE et le règlement (UE) no 1093/2010, et abrogeant la directive 2007/64/CE (JO L 337 du 23.12.2015, p. 35).

(10) Directive (UE) 2019/790 du Parlement européen et du Conseil du 17 avril 2019 sur le droit d'auteur et les droits voisins dans le marché unique numérique et modifiant les directives 96/9/CE et 2001/29/CE (JO L 130 du 17.5.2019, p. 92).

(11) Directive (UE) 2019/882 du Parlement européen et du Conseil du 17 avril 2019 relative aux exigences en matière d'accessibilité applicables aux produits et services (JO L 151 du 7.6.2019, p. 70).

(12) Directive 93/13/CEE du Conseil du 5 avril 1993 concernant les clauses abusives dans les contrats conclus avec les consommateurs (JO L 95 du 21.4.1993, p. 29).

(13) Directive (UE) 2015/1535 du Parlement européen et du Conseil du 9 septembre 2015 prévoyant une procédure d'information dans le domaine des réglementations techniques et des règles relatives aux services de la société de l'information (JO L 241 du 17.9.2015, p. 1).

(14) Directive (UE) 2018/1972 du Parlement européen et du Conseil du 11 décembre 2018 établissant le code des communications électroniques européen (JO L 321 du 17.12.2018, p. 36).

(15) Directive (UE) 2016/2102 du Parlement européen et du Conseil du 26 octobre 2016 relative à l'accessibilité des sites internet et des applications mobiles des organismes du secteur public (JO L 327 du 2.12.2016, p. 1).

(16) Règlement (UE) no 182/2011 du Parlement européen et du Conseil du 16 février 2011 établissant les règles et principes généraux relatifs aux modalités de contrôle par les États membres de l'exercice des compétences d'exécution par la Commission (JO L 55 du 28.2.2011, p. 13).

(17) Règlement (UE) 2018/1725 du Parlement européen et du Conseil du 23 octobre 2018 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union et à la libre circulation de ces données, et abrogeant le règlement (CE) no 45/2001 et la décision no 1247/2002/CE (JO L 295 du 21.11.2018, p. 39).

(18) Règlement (CE) no 1/2003 du Conseil du 16 décembre 2002 relatif à la mise en œuvre des règles de concurrence prévues aux articles 81 et 82 du traité (JO L 1 du 4.1.2003, p. 1).

(19) JO L 123 du 12.5.2016, p. 1.

(20) Directive (UE) 2019/1937 du Parlement européen et du Conseil du 23 octobre 2019 sur la protection des personnes qui signalent des violations du droit de l'Union (JO L 305 du 26.11.2019, p. 17).

(21) Directive (UE) 2020/1828 du Parlement européen et du Conseil du 25 novembre 2020 relative aux actions représentatives visant à protéger les intérêts collectifs des consommateurs et abrogeant la directive 2009/22/CE (JO L 409 du 4.12.2020, p. 1).

(22) JO C 147 du 26.4.2021, p. 4.

(23) Règlement (CE) no 139/2004 du Conseil du 20 janvier 2004 relatif au contrôle des concentrations entre entreprises («le règlement CE sur les concentrations») (JO L 24 du 29.1.2004, p. 1).

(24) Directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union (JO L 194 du 19.7.2016, p. 1).

ANNEXE

A. Généralités

1.

La présente annexe vise à préciser la méthode d'identification et de calcul des «utilisateurs finaux actifs» et des «entreprises utilisatrices actives» pour chaque service de plateforme essentiel énumérés à l'article 2, point 2). Elle fournit une référence permettant à une entreprise d'évaluer si ses services de plateforme essentiels respectent les seuils quantitatifs fixés à l'article 3, paragraphe 2, point b), et sont donc présumés satisfaire à l'exigence énoncée à l'article 3, paragraphe 1, point b). Cette référence sera donc également pertinente pour toute appréciation plus large au titre de l'article 3, paragraphe 8. Il incombe à l'entreprise de parvenir à la meilleure estimation possible, conformément aux principes communs et à la méthode spécifique énoncés dans la présente annexe. Aucune disposition de la présente annexe n'empêche la Commission, dans les délais fixés par les dispositions pertinentes du présent règlement, d'exiger de l'entreprise fournissant des services de plateforme essentiels qu'elle fournisse toutes les informations nécessaires pour identifier les «utilisateurs finaux actifs» et les «entreprises utilisatrices actives» et en calculer le nombre. Aucune disposition de la présente annexe ne devrait constituer une base juridique pour le traçage des utilisateurs. La méthode figurant dans la présente annexe est également sans préjudice de l'une quelconque des obligations fixées par le présent règlement, notamment celles énoncées à l'article 3, paragraphes 3 et 8, et à l'article 13, paragraphe 3. En particulier, le respect de l'article 13, paragraphe 3, signifie également qu'il convient d'identifier les «utilisateurs finaux actifs» et les «entreprises utilisatrices actives» et d'en calculer le nombre sur la base d'une mesure précise ou de la meilleure estimation possible, conformément aux capacités réelles d'identification et de calcul dont dispose au moment voulu l'entreprise fournissant des services de plateforme essentiels. Ces mesures ou la meilleure estimation possible doivent être cohérentes avec les informations communiquées en vertu de l'article 15 et les inclure.
2.

À l'article 2, les points 20) et 21) énoncent les définitions d'«utilisateur final» et d'«entreprise utilisatrice», qui sont communes à tous les services de plateforme essentiels.
3.

Afin d'identifier les «utilisateurs finaux actifs» et les «entreprises utilisatrices actives» et d'en calculer le nombre, la présente annexe fait référence à la notion d'«utilisateurs uniques». La notion d'«utilisateurs uniques» recouvre les «utilisateurs finaux actifs» et les «entreprises utilisatrices actives» comptabilisés une seule fois, pour le service de plateforme essentiel concerné, pour une période donnée (c'est-à-dire par mois dans le cas des «utilisateurs finaux actifs» et par année dans le cas des «entreprises utilisatrices actives»), indépendamment du nombre de leurs interactions avec le service de plateforme essentiel concerné au cours de cette période. Cela est sans préjudice du fait que la même personne physique ou morale peut simultanément constituer un «utilisateur final actif» ou une «entreprise utilisatrice active» pour différents services de plateforme essentiels.
B. «Utilisateurs finaux actifs»

1.

Le nombre d'«utilisateurs uniques» au regard des «utilisateurs finaux actifs» est établi en fonction de la mesure la plus précise déclarée par l'entreprise fournissant l'un des services de plateforme essentiels, en particulier:
a)

On considère que la collecte de données sur l'utilisation des services de plateforme essentiels à partir d'environnements fonctionnant par inscription ou connexion présenterait, à première vue, le risque le plus faible de duplication, par exemple concernant le comportement des utilisateurs sur l'ensemble des appareils ou des plateformes. Par conséquent, l'entreprise soumet des données anonymisées agrégées sur le nombre d'utilisateurs finaux uniques par service de plateforme essentiel concerné sur la base des environnements fonctionnant par inscription ou connexion, si de telles données existent.

b)

Dans le cas des services de plateforme essentiels auxquels des utilisateurs finaux ont également accès en dehors des environnements fonctionnant par inscription ou connexion, l'entreprise soumet en outre des données anonymisées agrégées sur le nombre d'utilisateurs finaux uniques du service de plateforme essentiel concerné, sur la base d'une autre mesure prenant en compte également les utilisateurs finaux en dehors des environnements fonctionnant par inscription ou connexion, tels que les adresses de protocole internet, les témoins de connexion (cookies) ou d'autres identifiants tels que les étiquettes d'identification par radiofréquence, pour autant que ces adresses ou témoins de connexion soient objectivement nécessaires à la fourniture de services de plateforme essentiels.

2.

Le nombre d'«utilisateurs finaux actifs par mois» est fondé sur le nombre moyen d'utilisateurs finaux actifs chaque mois durant la majeure partie de l'exercice. La notion de «majeure partie de l'exercice» vise à permettre à une entreprise fournissant des services de plateforme essentiels d'écarter des valeurs exceptionnelles au cours d'une année donnée. On entend par valeurs exceptionnelles celles qui sortent nettement de ce qui ressort de l'ordinaire

et du prévisible. Une situation où, de manière inattendue, au cours d'un seul mois de l'exercice, la participation des utilisateurs atteindrait un niveau record ou connaîtrait une forte baisse est un exemple de ce qui pourrait constituer de telles valeurs exceptionnelles. Les valeurs en rapport avec des événements intervenant chaque année, tels que les promotions annuelles des ventes, ne constituent pas des valeurs exceptionnelles.

C. «Entreprises utilisatrices actives»

Le nombre d'«utilisateurs uniques» au regard des «entreprises utilisatrices actives» doit être déterminé, s'il y a lieu, au niveau du compte, chaque compte d'entreprise distinct, associé à l'utilisation d'un service de plateforme essentiel fourni par l'entreprise, constituant une entreprise utilisatrice unique de ce service de plateforme essentiel. Si la notion de «compte d'entreprise» ne s'applique pas à un service de plateforme essentiel donné, l'entreprise concernée fournissant des services de plateforme essentiels détermine le nombre d'entreprises utilisatrices uniques en se référant à l'entreprise concernée.

D. Communication d'informations

1.

L'entreprise qui communique à la Commission, conformément à l'article 3, paragraphe 3, des informations concernant le nombre d'utilisateurs finaux actifs et d'entreprises utilisatrices actives par service de plateforme essentiel est chargée de veiller à l'exhaustivité et à l'exactitude de ces informations. À cet égard:

a)

l'entreprise est tenue de transmettre les données pour un service de plateforme essentiel donné en évitant de sous-évaluer ou de surévaluer le nombre d'utilisateurs finaux actifs et d'entreprises utilisatrices actives (par exemple, lorsque les utilisateurs accèdent aux services de plateforme essentiels à partir de différentes plateformes ou de différents appareils);

b)

l'entreprise est tenue de fournir des explications précises et succinctes sur la méthode utilisée pour obtenir les informations fournies et elle est responsable de tout risque de sous-évaluation ou de surévaluation du nombre d'utilisateurs finaux actifs et d'entreprises utilisatrices actives pour un service de plateforme essentiel donné et des solutions adoptées pour remédier à ce risque;

c)

l'entreprise fournit des données basées sur une autre méthode de mesure lorsque la Commission a des doutes quant à l'exactitude des données fournies par l'entreprise fournissant les services de plateforme essentiels.

2.

Aux fins du calcul du nombre d'«utilisateurs finaux actifs» et d'«entreprises utilisatrices actives»:

a)

l’entreprise fournissant un ou des services de plateforme essentiels ne répertorie pas les services de plateforme essentiels appartenant à une même catégorie de services de plateforme essentiels définis à l’article 2, point 2), comme étant distincts en se basant principalement sur le fait qu’ils sont fournis en utilisant des noms de domaine différents, qu’il s’agisse de domaines de premier niveau nationaux (ccTLD) ou de domaines de premier niveau génériques (gTLD), ou sur tout attribut géographique;

b)

l’entreprise fournissant un ou des services de plateforme essentiels considère comme distincts les services de plateforme essentiels qui sont utilisés à des fins différentes soit par leurs utilisateurs finaux, soit par leurs entreprises utilisatrices, soit encore par les deux, même si leurs utilisateurs finaux ou leurs entreprises utilisatrices peuvent être identiques et même s’ils appartiennent à la même catégorie de services de plateforme essentiels définis à l’article 2, point 2);

c)

l’entreprise fournissant un ou des services de plateforme essentiels considère comme étant des services de plateforme essentiels distincts les services que l’entreprise concernée propose de manière intégrée, mais qui:

i)

n’appartiennent pas à la même catégorie de services de plateforme essentiels définis à l’article 2, point 2), ou

ii)

sont utilisés à des fins différentes soit par leurs utilisateurs finaux, soit par leurs entreprises utilisatrices, soit encore par les deux, même si leurs utilisateurs finaux ou leurs entreprises utilisatrices peuvent être identiques et même s’ils appartiennent à la même catégorie de services de plateforme essentiels en vertu de l’article 2, point 2).

E. «Définitions spécifiques»

Le tableau ci-dessous contient des définitions spécifiques des notions d’«utilisateurs finaux actifs» et d’«entreprises utilisatrices actives» pour chaque service de plateforme essentiel.

Services de plateforme essentiels

Utilisateurs finaux actifs

Entreprises utilisatrices actives

Services d’intermédiation en ligne

Nombre d’utilisateurs finaux uniques qui, au moins une fois pendant le mois, ont interagi avec le service d’intermédiation en ligne, par exemple en se connectant, en effectuant une

recherche, en cliquant ou en utilisant le défilement de manière active, ou qui, au moins une fois pendant le mois, ont conclu une transaction via le service d'intermédiation en ligne.

Nombre d'entreprises utilisatrices uniques dont au moins un article a figuré sur une liste dans le service d'intermédiation en ligne pendant toute l'année ou qui, pendant l'année, ont conclu une transaction rendue possible par le service d'intermédiation en ligne.

Moteurs de recherche en ligne

Nombre d'utilisateurs finaux uniques qui, au moins une fois pendant le mois, ont interagi avec le moteur de recherche en ligne, par exemple en effectuant une recherche.

Nombre d'entreprises utilisatrices uniques disposant de sites internet commerciaux (c'est-à-dire de sites internet utilisés à des fins commerciales ou professionnelles) qui sont indexés par le moteur de recherche en ligne ou font partie de l'index du moteur de recherche en ligne pendant l'année.

Services de réseaux sociaux en ligne

Nombre d'utilisateurs finaux uniques qui ont interagi avec le service de réseau social en ligne au moins une fois pendant le mois, par exemple en se connectant, en ouvrant une page, en utilisant le défilement, en cliquant, en utilisant la fonction «Like/J'aime», en lançant une recherche, en publiant ou en commentant, de manière active.

Nombre d'entreprises utilisatrices uniques qui sont inscrites sur la liste d'entreprises ou disposent d'un compte d'entreprise dans le service de réseau social en ligne et qui ont interagi avec le service, de quelque manière que ce soit, au moins une fois pendant l'année, par exemple en se connectant, en ouvrant une page, en utilisant le défilement, en cliquant, en utilisant la fonction «Like/J'aime», en effectuant une recherche, en publiant, en commentant ou en utilisant ses outils pour les entreprises, de manière active.

Services de plateformes de partage de vidéos

Nombre d'utilisateurs finaux uniques qui ont interagi avec le service de plateforme de partage de vidéos au moins une fois pendant le mois, par exemple en diffusant un segment de contenu audiovisuel, en effectuant une recherche ou en téléchargeant un contenu audiovisuel vers la plateforme, y compris des vidéos créées par les utilisateurs.

Nombre d'entreprises utilisatrices uniques qui, pendant l'année, ont fourni au moins un contenu audiovisuel téléchargé vers le service de la plateforme de partage de vidéos ou diffusé sur celle-ci.

Services de communications interpersonnelles non fondés sur la numérotation

Nombre d'utilisateurs finaux uniques qui, au moins une fois pendant le mois, ont lancé d'une manière ou d'une autre une communication ou y ont participé par l'intermédiaire du service de communications interpersonnelles non fondé sur la numérotation.

Nombre d'entreprises utilisatrices uniques qui, au moins une fois pendant l'année, ont utilisé un compte d'entreprise ou qui ont, de n'importe quelle autre manière, lancé une

communication ou, de quelque façon que ce soit, y ont participé par l'intermédiaire du service de communication interpersonnelle non fondé sur la numérotation pour communiquer directement avec un utilisateur final.

Systèmes d'exploitation

Nombre d'utilisateurs finaux uniques qui ont utilisé un dispositif équipé du système d'exploitation ayant été activé, mis à jour ou utilisé au moins une fois pendant le mois.

Nombre de développeurs uniques qui, pendant l'année, ont publié, mis à jour ou proposé au moins une application ou un programme logiciel utilisant le langage de programmation ou tout outil de développement logiciel du système d'exploitation ou fonctionnant de quelque manière que ce soit sur le système d'exploitation.

Assistant virtuel

Nombre d'utilisateurs finaux uniques qui, au moins une fois pendant le mois, ont interagi avec l'assistant virtuel de quelque manière que ce soit, par exemple en l'activant, en posant une question, en accédant à un service par une commande ou en contrôlant un dispositif de maison intelligente.

Nombre de développeurs uniques qui, au cours de l'année, ont proposé au moins une application logicielle d'assistant virtuel ou une fonctionnalité permettant de rendre une application logicielle existante accessible par l'intermédiaire de l'assistant virtuel.

Navigateurs internet

Nombre d'utilisateurs finaux uniques qui, au moins une fois pendant le mois, ont interagi avec le navigateur internet, par exemple en insérant une requête ou une adresse de site internet dans la ligne URL du navigateur internet.

Nombre d'entreprises utilisatrices uniques dont les sites internet d'entreprise (c'est-à-dire les sites internet utilisés à des fins commerciales ou professionnelles) ont, au moins une fois pendant le mois, été consultés par l'intermédiaire du navigateur internet ou qui ont proposé un plug-in, une extension ou des outils complémentaires utilisés sur le navigateur internet au cours de l'année.

Services d'informatique en nuage

Nombre d'utilisateurs finaux uniques qui, au moins une fois pendant le mois, ont interagi avec des services d'informatique en nuage fournis par le fournisseur concerné de services d'informatique en nuage, en échange de tout type de rémunération, que celle-ci ait eu lieu ou non le même mois.

Nombre d'entreprises utilisatrices uniques qui, au cours de l'année, ont fourni tout service d'informatique en nuage hébergé dans l'infrastructure en nuage du fournisseur de services d'informatique en nuage concerné.

Services de publicité en ligne

Pour les ventes propriétaires d’espaces publicitaires:

Nombre d’utilisateurs finaux uniques qui, au moins une fois pendant le mois, ont été exposés à une publicité.

Pour les services d’intermédiation publicitaire (y compris les réseaux publicitaires, les échanges publicitaires et tout autre service d’intermédiation publicitaire):

Nombre d’utilisateurs finaux uniques qui, au moins une fois pendant le mois, ont été exposés à une publicité ayant déclenché le service d’intermédiation publicitaire.

Pour les ventes propriétaires d’espaces publicitaires:

Nombre d’annonceurs uniques dont au moins une publicité a été exposée pendant l’année.

Pour les services d’intermédiation publicitaire (y compris les réseaux publicitaires, les échanges publicitaires et tout autre service d’intermédiation publicitaire):

Nombre d’entreprises utilisatrices uniques (y compris les annonceurs, les éditeurs ou d’autres intermédiaires) qui, au cours de l’année, ont interagi via le service d’intermédiation publicitaire ou ont eu recours à ses services.