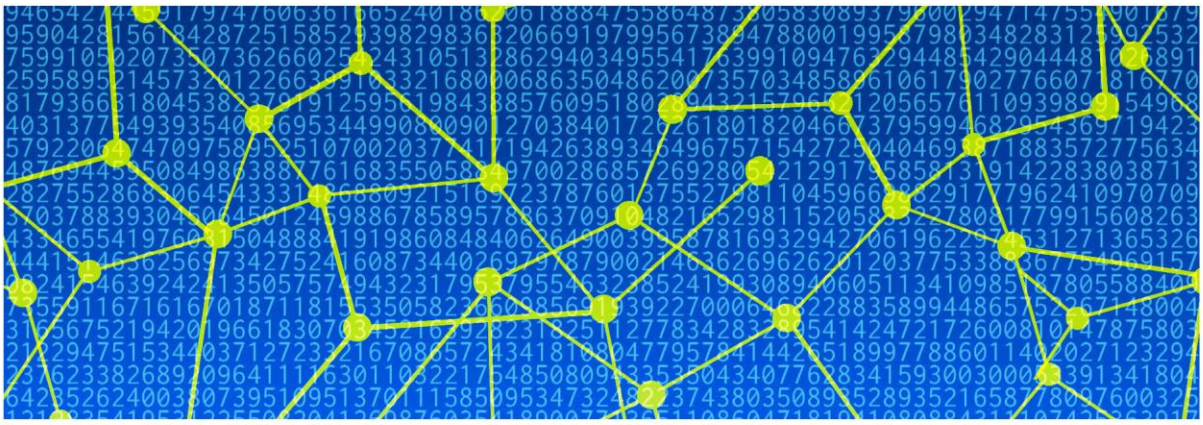

EUROPEAN DATA PROTECTION SUPERVISOR

Avis nº 02/2021

concernant la proposition de législation sur les marchés numériques

EDPS

Le Contrôleur européen de la protection des données (CEPD) est une institution indépendante de l'Union européenne chargée, en vertu de l'article 52, paragraphe 2, du règlement (UE) 2018/1725, «[e]n ce qui concerne le traitement de données à caractère personnel, [...] de veiller à ce que les libertés et droits fondamentaux des personnes physiques, notamment le droit à la protection des données, soient respectés par les institutions et organes de l'Union» et, en vertu de l'article 52, paragraphe 3, «de conseiller les institutions et organes de l'Union et les personnes concernées pour toutes les questions concernant le traitement des données à caractère personnel».

Wojciech Wiewiorówski a été nommé Contrôleur le 5 décembre 2019 pour un mandat de cinq ans.

En vertu de l'article 42, paragraphe 1, du règlement (UE) 2018/1725, «[à] la suite de l'adoption de propositions d'acte législatif, de recommandations ou de propositions au Conseil en vertu de l'article 218 du traité sur le fonctionnement de l'Union européenne ou lors de l'élaboration d'actes délégués ou d'actes d'exécution, la Commission consulte le Contrôleur européen de la protection des données en cas d'incidence sur la protection des droits et libertés des personnes physiques à l'égard du traitement des données à caractère personnel», et de l'article 57, paragraphe 1, point g), dudit règlement, le CEPD «conseille, de sa propre initiative ou sur demande, l'ensemble des institutions et organes de l'Union sur les mesures législatives et administratives relatives à la protection des droits et libertés des personnes physiques à l'égard du traitement des données à caractère personnel».

Le présent avis est rendu par le CEPD dans le délai de huit semaines à compter de la réception de la demande de consultation prévue à l'article 42, paragraphe 3, du règlement (UE) 2018/1725, compte tenu de l'incidence sur la protection des droits et des libertés des personnes à l'égard du traitement des données à caractère personnel de la proposition de règlement du Parlement européen et du Conseil relatif aux marchés contestables et équitables dans le secteur numérique (législation sur les marchés numériques), adoptée par la Commission européenne.

Synthèse

Le 15 décembre 2020, la Commission a publié une proposition de règlement du Parlement européen et du Conseil relatif aux marchés contestables et équitables dans le secteur numérique (**législation sur les marchés numériques**). La proposition fait suite à la **Communication intitulée *Façonner l'avenir numérique de l'Europe***, dans laquelle il est indiqué que des règles supplémentaires peuvent être nécessaires pour garantir la **contestabilité, l'équité et l'innovation et la possibilité d'entrée sur le marché**, ainsi que des intérêts publics qui vont au-delà de la concurrence ou de considérations économiques. La proposition établit des règles ex ante afin que les marchés caractérisés par de grandes plateformes générant des effets de réseau importants («contrôleurs d'accès») restent équitables et contestables.

Ce faisant, la proposition établit les dispositions relatives à **la désignation des contrôleurs d'accès** tenant compte de l'avantage tiré des données en ce qui concerne notamment l'accès aux données à caractère personnel et la collecte de ces données par le fournisseur; **les obligations et interdictions** auxquelles les contrôleurs d'accès sont soumis; les règles pour la conduite d'**enquêtes sur le marché**; les dispositions relatives **à la mise en œuvre et à l'application** de la proposition.

Dans cet avis, le CEPD **accueille favorablement la proposition,** dans la mesure où elle vise à promouvoir des **marchés équitables et ouverts et le traitement équitable des données à caractère personnel**. Dès 2014, le CEPD a souligné que **le droit de la concurrence, de la protection des consommateurs et de la protection des données sont trois domaines d'action inextricablement liés** dans le contexte de **l'économie des plateformes en ligne**. Le CEPD estime que la relation entre ces trois domaines devrait être une relation de **complémentarité**, et non une relation dans laquelle un domaine se substitue à un autre ou entre en conflit avec un autre.

Dans le présent avis, le CEPD met en évidence les dispositions de la proposition qui ont pour effet de **renforcer mutuellement** la contestabilité du marché et, en fin de compte, le contrôle par la personne concernée de ses données à caractère personnel. C'est notamment le cas de l'**article 5, point f)**, qui interdit d'exiger des utilisateurs finaux qu'ils s'abonnent à d'autres services de plateforme essentiels proposés par le contrôleur d'accès; de **l'article 6, paragraphe 1, point b)**, qui permet à l'utilisateur final de désinstaller des applications logicielles préinstallées dans le service de plateforme essentiel; de **l'article 6, paragraphe 1, point e)**, qui interdit au contrôleur d'accès de restreindre la capacité des utilisateurs finaux de passer à d'autres applications logicielles et services; et de l'**article 13**, qui prévoit l'obligation pour le contrôleur d'accès de soumettre à la Commission une description, devant faire 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.

Par ailleurs, le CEPD formule des **recommandations spécifiques** visant à s'assurer que la proposition **complète efficacement le RGPD,** en renforçant la protection des libertés et droits fondamentaux des personnes concernées et **en évitant les conflits** avec les règles actuelles en matière de protection des données. À cet égard, le CEPD recommande plus particulièrement de préciser à **l'article 5, point a)** de la proposition que le contrôleur d'accès propose aux utilisateurs finaux une solution d'accessibilité facile et rapide pour la gestion du consentement; de préciser le champ d'application de la portabilité des données prévue à **l'article 6, paragraphe 1, point h)** de la proposition; de reformuler **l'article 6, paragraphe 1, point i)** de la proposition pour garantir la pleine conformité avec le RGPD; et d'attirer l'attention sur la nécessité d'une **anonymisation**

effective et de tests de ré-identification lors du partage des données concernant les requêtes, clics et vues en lien avec les recherches gratuites et payantes générées par les utilisateurs finaux sur les moteurs de recherche en ligne du contrôleur d'accès.

En outre, le CEPD invite les colégislateurs à envisager d'introduire des **exigences minimales d'interopérabilité** pour les contrôleurs d'accès et à promouvoir l'élaboration de normes techniques au niveau européen, conformément à la législation de l'Union applicable en matière de normalisation européenne.

Enfin, en s'appuyant notamment sur l'expérience de la Digital Clearinghouse, le CEPD recommande de préciser, à l'**article 32, paragraphe 1**, que le **comité consultatif en matière de marchés numériques** comprend des représentants du comité européen de la protection des données, et demande, plus largement, de mettre en place une **coopération institutionnalisée et structurée** entre les autorités de contrôle compétentes concernées, y compris les autorités chargées de la protection des données. Cette coopération devrait notamment permettre d'échanger toutes les informations pertinentes avec les autorités compétentes afin qu'elles puissent remplir leur rôle complémentaire, tout en agissant conformément à leur mandat institutionnel respectif.

TABLE DES MATIÈRES

1 Table des matières

LE CONTRÔLEUR EUROPÉEN DE LA PROTECTION DES DONNÉES,

vu le traité sur le fonctionnement de l'Union européenne, et notamment son article 16,

vu la charte des droits fondamentaux de l'Union européenne (la «charte»), et notamment ses articles 7 et 8,

vu le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)[1],

vu la 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»)[2],

vu le 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[3], et notamment son article 42, paragraphe 1,

A ADOPTÉ LE PRÉSENT AVIS:

1. INTRODUCTION ET CONTEXTE

1. Le 15 décembre 2020, la Commission européenne a adopté la proposition de règlement du Parlement européen et du Conseil relatif aux marchés contestables et équitables dans le secteur numérique (législation sur les marchés numériques) (ci-après la «proposition»)[4].

2. La proposition fait suite à la **Communication intitulée *Façonner l'avenir numérique de l'Europe***, dans laquelle il était indiqué que des règles supplémentaires peuvent être nécessaires pour garantir la contestabilité, l'équité et l'innovation du marché et la possibilité d'entrée sur le marché, ainsi que les intérêts publics qui vont au-delà de la concurrence ou de considérations économiques. La communication annonçait également que la Commission étudierait la possibilité d'instaurer des règles ex ante afin que les marchés caractérisés par de grandes plateformes générant des effets de réseau importants et agissant en tant que «gardiens» restent équitables et contestables pour les innovateurs, les entreprises et les nouveaux entrants[5].

3. Selon **l'exposé des motifs** de la proposition, quelques grandes plateformes du secteur numérique jouent de plus en plus le rôle de points d'accès ou de «contrôleurs d'accès» entre les entreprises utilisatrices et les utilisateurs finaux. Ces contrôleurs d'accès seraient ancrés dans les marchés numériques, ce qui entraîne une forte dépendance pour de nombreuses entreprises utilisatrices et provoque des effets négatifs sur la contestabilité des services de plateforme essentiels concernés. Dans certains cas, la dépendance occasionne un comportement déloyal à l'égard des entreprises utilisatrices[6].

4. L'**objectif de la proposition** est de traiter au niveau de l'UE les cas les plus marquants de pratiques déloyales et la faible contestabilité concernant ce qu'il convient d'appeler les «services de plateforme essentiels»[7]. À cette fin, la proposition:

- fixe les conditions selon lesquelles les fournisseurs de services de plateforme essentiels doivent être désignés comme «contrôleurs d'accès» (chapitre II);
- décrit les pratiques déloyales des contrôleurs d'accès qui limitent la contestabilité, définissant les obligations que les contrôleurs d'accès désignés doivent respecter, dont certaines sont susceptibles d'être précisées (chapitre III);
- prévoit des règles pour la conduite des enquêtes sur le marché (chapitre IV); et
- contient les dispositions relatives à la mise en œuvre et à l'application du présent règlement (chapitre V).

5. Le CEPD a été consulté de manière informelle sur le projet de proposition de législation sur les marchés numériques le 8 décembre 2020. Le CEPD se félicite d'avoir été consulté à ce stade précoce de la procédure.

6. En plus de la proposition, la Commission a également adopté une proposition de règlement du Parlement européen et du Conseil relatif à un marché intérieur des services numériques (législation sur les services numériques) et modifiant la directive 2000/31/CE. Conformément à l'article 42, paragraphe 1, du règlement (UE) 2018/1725, le CEPD a aussi été consulté sur la proposition de législation sur les services numériques, qui fait l'objet d'un avis distinct.

2. OBSERVATIONS GÉNÉRALES

7. Le CEPD rappelle que l'avenir numérique de l'Europe est au cœur de la Stratégie du CEPD pour 2020-2024, qui vise à façonner une Europe numérique plus sûre, plus équitable et plus durable, en particulier pour les personnes les plus vulnérables de nos sociétés[8].

8. Le CEPD soutient l'objectif de la Commission visant à garantir **l'équité et la contestabilité** des marchés dans le secteur numérique, en particulier en ce qui concerne les services de plateforme essentiels. Le CEPD se félicite aussi de la reconnaissance du fait que des règles supplémentaires peuvent être nécessaires pour garantir les intérêts publics qui vont au-delà de la concurrence ou de considérations économiques, en plus de la nécessité de garantir l'innovation et l'entrée sur le marché[9].

9. Le CEPD se félicite tout particulièrement que la proposition reconnaisse explicitement que «*[l]es 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*»[10].

10. Le CEPD est également conscient que la nécessité d'une «mise à jour numérique» du droit de la concurrence a fait l'objet de débats approfondis non seulement dans l'UE, mais aussi au niveau mondial, y compris au Royaume-Uni[11] et aux États-Unis[12].

11. Compte tenu du modèle commercial de certaines plateformes (désignées ci-après par «contrôleurs d'accès»), la proposition comprend nécessairement des règles (ex ante) qui visent en outre à promouvoir des **marchés équitables et ouverts et le traitement équitable des données àcaractère personnel**.

12. Dès 2014, le CEPD a souligné que le droit de la concurrence, de la protection des consommateurs et de la protection des données sont trois domaines d'action

inextricablement liés dans le contexte de l'économie des plateformes en ligne[13]. Le CEPD estime que la relation entre ces trois domaines devrait être une relation de complémentarité, de convergence et d'application cohérente, et non une relation dans laquelle un domaine se substitue à un autre ou entre en conflit avec un autre.

13. Les services en ligne sont devenus dépendants d'un suivi souvent clandestin de personnes, qui n'ont généralement pas conscience de la nature et de l'étendue de ce suivi[14]. Ce modèle commercial prédominant est souvent associé aux tendances de l'économie numérique qui se situent à la croisée de ces différents domaines législatifs. Ces derniers comprennent: l'asymétrie de l'information et du pouvoir entre les grandes plateformes et les personnes; une transparence et une responsabilité insuffisantes; une inégalité croissante dans la répartition de la valeur; des comportements de manipulation et de dépendance; des plateformes en tant que contrôleurs d'accès pour des solutions, un choix, et l'innovation, la manipulation en ligne et la désinformation[15].

14. Par conséquent, le CEPD se félicite de la déclaration selon laquelle la proposition vise à **compléter** les lois sur la protection des données, notamment en *complétant* le niveau de protection existant et en *contribuant à éclairer l'application* du règlement général sur la protection des données («RGPD»)[16]. Compte tenu de la complémentarité des objectifs poursuivis, le CEPD soutient pleinement les objectifs de la proposition.

15. Dans les paragraphes qui suivent, le CEPD formule des recommandations spécifiques visant à s'assurer que la proposition **complète efficacement leRGPD** et **renforce la protection** des libertés et droits fondamentaux des personnes concernées et évite les **conflits** avec les règles actuelles en matière de protection des données.

3. RECOMMANDATIONS SPÉCIFIQUES

3.1. Objet et champ d'application

16. Le considérant 11 de la proposition confirme que le règlement devrait «compléter» et qu'il est «sans préjudice» de l'application du règlement (UE) 2016/679[17]. Dans un souci de clarté, le CEPD recommande de préciser que la proposition complète le règlement 2016/679 **et la directive 2002/58/CE.** Il conviendrait également de préciser dans le considérant que la proposition **ne précise ni ne remplace** aucune des obligations des services de plateforme essentiels en vertu du règlement 2016/679 et de la directive 2002/58/CE.

17. Le CEPD recommande de compléter **l'article 1er** de la proposition afin de refléter le libellé du considérant 11, en indiquant explicitement que la proposition **complète** le règlement (UE) 2016/679 et la directive 2002/58/CE **et s'entend sans préjudice de ceux-ci**[18].

3.2. Définitions

18. Le CEPD note que l'article 2 de la proposition fait référence, à juste titre, à plusieurs définitions prévues par le RGPD («données à caractère personnel»[19]; «données à caractère non personnel»[20]), plutôt que d'introduire d'autres définitions qui pourraient créer de l'ambiguïté ou des difficultés d'interprétation.

19. Le CEPD note toutefois que la proposition contient des exigences faisant référence à des concepts déjà définis et utilisés par le règlement 2016/679 et/ou la directive 2002/58, tels que

le «profilage»[21], le «consentement»[22] et la «portabilité des données»[23]. Par conséquent, des précisions supplémentaires sont nécessaires pour éviter toute confusion (au-delà de la mention selon laquelle le présent règlement est «sans préjudice» de l'application du RGPD).

20. En particulier, le CEPD fait valoir que, dans un souci de clarté, le terme «profilage» visé à l'article 13 de la proposition devrait avoir la même signification que le «profilage» défini à l'article 4, paragraphe 4, du RGPD, et suggère d'ajouter à l'article 2 de la proposition («définitions») une référence spécifique à la définition du «profilage» telle que visée à l'article 4, paragraphe 4, du RGPD en ce qui concerne le profilage des utilisateurs finaux ou des consommateurs.

    En ce qui concerne la référence au «consentement», à l'article 5, point a), à l'article 6, paragraphe 1, point i) et à l'article 11, paragraphe 2, la proposition précise qu'il s'agit d'un consentement «conforme au règlement 2016/679». Le CEPD suggère d'ajouter à l'article 2 de la proposition («Définitions») une référence spécifique à la définition du «consentement» telle que visée à l'article 4, paragraphe 11, du RGPD en ce qui concerne le consentement des utilisateurs finaux.

    Le CEPD suggère également d'apporter des précisions supplémentaires en ce qui concerne la «portabilité des données» visée à l'article 6, paragraphe 1, point h), de la proposition, qui sont expliquées plus loin dans le présent avis (voir paragraphe 29 ci-dessous).

3.3. Désignation des contrôleurs d'accès

21. Parmi les éléments pertinents pour la désignation des «contrôleurs d'accès», le CEPD se félicite de la référence aux «***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 le fournisseur, ou les capacités d'analyse de ce dernier***» [article 3, paragraphe 6, point c)[24]] ainsi qu'à «***la captivité des utilisateurs finaux***»[article 3, paragraphe 6, point e)][25]. En effet, le CEPD considère que les plateformes en ligne qui, en tant que composante essentielle de leur modèle commercial, s'engagent dans le profilage des individus, peuvent tirer des avantages concurrentiels considérables en raison de leur capacité unique à collecter d'importants volumes et types de données à caractère personnel. La captivité des utilisateurs peut également permettre aux contrôleurs d'accès d'augmenter les prix pour les consommateurs, y compris les prix non monétaires, ce qui peut entraîner une éventuelle dégradation du niveau de protection des données à caractère personnel pour les utilisateurs finaux.

3.4. Pratiques des contrôleurs d'accès qui limitent la contestabilité et sont déloyales

22. Compte tenu des barrières à l'entrée qui résultent de l'avantage tiré des données, mais aussi (indirectement) de la captivité de l'utilisateur, **l'article 5, point a),** de la proposition prévoit que le contrôleur d'accès:

    «s'abstient de ***combiner sources de données à caractère personnel provenant de ces services de plateforme essentiels avec les données à caractère personnel provenant de tout autre service proposé par le contrôleur d'accès, ou avec les données à caractère personnel provenant de services tiers****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*** *n'ait été laissé à l'utilisateur final et que ce dernier* ***ait donné son consentement au sens du règlement (UE) 2016/679****».*

Le considérant 36 précise que «*[l]e comportement consistant à combiner des données d'utilisateurs finaux provenant de différentes sources ou à inscrire des utilisateurs à différents services des contrôleurs d'accès confère à ces derniers des avantages potentiels en ce qui concerne l'accumulation de données, érigeant de ce fait des barrières à l'entrée. Afin d'éviter que la contestabilité des services de plateforme essentiels ne soit injustement compromise par les contrôleurs d'accès, ceux-ci devraient permettre à leurs utilisateurs finaux de* ***choisir librement d'adhérer*** *à de telles pratiques commerciales en proposant une autre possibilité moins personnalisée. Cette possibilité devrait couvrir toutes les sources possibles de données à caractère personnel, y compris les propres services des contrôleurs d'accès ainsi que les sites web de tiers, et devrait être présentée à l'utilisateur final de manière proactive, explicite, claire et simple.*»

23. Le CEPD **se félicite** de cette disposition, car elle contribue à résoudre les problèmes de concurrence et renforce davantage encore la protection des droits fondamentaux à la vie privée et à la protection des données à caractère personnel en ce qui concerne les contrôleurs d'accès.

24. Toutefois, dans un souci de clarté, le CEPD rappelle que les plateformes en ligne qui ne sont pas désignées comme des «contrôleurs d'accès» peuvent encore avoir besoin d'obtenir le consentement des personnes concernées avant de combiner des données entre leurs services ou avec des données provenant de services tiers conformément au RGPD et/ou à la directive «vie privée et communications électroniques». L'article 5, point a), ne devrait donc pas être interprété comme suggérant que les plateformes qui ne sont **pas désignées comme des contrôleurs d'accès** peuvent librement combiner des données à caractère personnel entre services sans le consentement de l'intéressé[26]. Le CEPD recommande d'ajouter une précision à cet effet dans un considérant.

25. Le CEPD recommande de préciser que le contrôleur d'accès fournit aux utilisateurs finaux **une solution conviviale** (d'accessibilité facile et rapide) pour la gestion du consentement, conformément au règlement 2016/679, et en particulier l'exigence de protection des données dès la conception et de protection des données par défaut énoncée à l'article 25 du règlement 2016/679. À titre d'exemple, la proposition pourrait préciser que les fonctionnalités permettant de fournir des informations et d'offrir la possibilité d'accorder, de modifier ou de révoquer le consentement devraient être aussi conviviales que possible.

26. Le CEPD se félicite également de **l'article 5, point f),** de la proposition, qui **interdit** au contrôleur d'accès d'exiger de l'entreprise utilisatrice ou des utilisateurs finaux **qu'ils s'abonnent ou s'enregistrent à tout autre service de plateforme essentiel proposé par le contrôleur d'accès**. Cette disposition peut atténuer les problèmes de concurrence (sur le «**regroupement obligatoire des services**») et réduire la collecte et la combinaison excessives de données à caractère personnel.

    Le CEPD estime que si l'article 5, point f), de la proposition **renforce indirectement les garanties** en matière de protection des données et de respect de la vie privée, il le fait sans empiéter sur le RGPD, étant donné que cette exigence est également justifiée par la position particulière du contrôleur d'accès et par le fonctionnement de l'économie des plateformes.

27. Le CEPD fait observer que le raisonnement qui sous-tend l'article 5, point f), s'appliquerait également à l**'article 5, point e)**, qui interdit au contrôleur d'accès d'exiger de l'entreprise utilisatrice (mais pas de l'utilisateur final) **qu'elle utilise, propose ou interagisse avec un service d'identification du contrôleur d'accès** dans le cadre des services qu'elle propose en

ayant recours aux services de plateforme essentiels de ce contrôleur d'accès. Par conséquent, le CEPD recommande d'insérer les termes «**ou des utilisateurs finaux**» après «entreprises utilisatrices» à l'article 5, point e).

28. Le CEPD fait observer que les dispositions suivantes démontrent de manière similaire que le droit de la concurrence et le droit relatif à la protection des données peuvent utilement se compléter et se renforcer mutuellement:

    - **l'article 6, paragraphe 1, point a)**, qui prévoit que le contrôleur d'accès «*s'abstient d'utiliser, en concurrence avec les entreprises utilisatrices de ses services de plateforme essentiels, les données quelles qu'elles soient non accessibles au public qui sont générées par les activités de ces entreprises utilisatrices, y compris par leurs utilisateurs finaux, ou qui sont fournies par ces entreprises utilisatrices ou par leurs utilisateurs finaux*»;

    - **l'article 6, paragraphe 1, point b)**, qui prévoit que le contrôleur d'accès «*permet aux utilisateurs finaux de **désinstaller** toute application logicielle préinstallée dans son service de plateforme essentiel* (..)»;

    - **l'article 6, paragraphe 1, point e)**, qui prévoit que le contrôleur d'accès «*s'abstient de restreindre techniquement la capacité des utilisateurs finaux **de passer** et de s'abonner à d'autres applications logicielles et services accessibles par le système d'exploitation du contrôleur d'accès, y compris en ce qui concerne le choix du fournisseur d'accès à l'internet pour les utilisateurs finaux*».

29. **L'article 6, paragraphe 1, point h)**, de la proposition dispose que le contrôleur d'accès: «*assure la **portabilité effective** des données générées par l'activité d'une entreprise utilisatrice ou d'un utilisateur final et, en particulier, fournit aux utilisateurs finaux les outils facilitant l'exercice de cette portabilité, conformément au règlement (UE) 2016/679, dont la fourniture d'un accès continu et en temps réel*».

    Le CEPD rappelle qu'en vertu de l'article 20 du RGPD, le droit à la portabilité des données inclut le droit de la personne concernée de recevoir les données à caractère personnel la concernant, qu'elle a fournies à un responsable du traitement, et le droit de transmettre ces données à un autre responsable du traitement. Ainsi que l'a précisé le groupe de travail «article 29» et comme l'a confirmé ultérieurement le comité européen de la protection des données[27], **le champ d'application** des données à caractère personnel qui pourraient être concernées par la «portabilité» englobe les données à caractère personnel fournies sciemment et activement par la personne concernée, **ainsi que les données à caractère personnel générées par son activité** (pour autant que la base juridique du traitement soit le consentement ou le contrat, ce qui est susceptible d'être le cas en l'espèce). Par conséquent, le CEPD se félicite également de la référence aux «données générées par l'activité d'un [...] utilisateur final» à l'article 6, paragraphe 1, point h), de la proposition.

    Le CEPD considère toutefois que l'article 6, paragraphe 1, point h), devrait être formulé de manière plus précise pour mentionner les personnes qui seraient habilitées à transférer des données à caractère personnel et les données, à caractère personnel ou non, qui feraient l'objet de la portabilité. Le CEPD recommande de préciser que, en ce qui concerne la portabilité des données à destination des utilisateurs finaux, un contrôleur d'accès fournit à l'utilisateur final des **outils** facilitant la portabilité effective des **données à caractère personnel le concernant, y compris les données à caractère personnel générées par son activité en tant qu'utilisateur final** de services de plateforme conformément à l'article 20 du règlement 2016/679, y compris par la fourniture d'un accès continu et en temps réel.

30. **L'article 6, paragraphe 1, point i),** de la proposition prévoit que le contrôleur d'accès «*procure gratuitement aux entreprises utilisatrices, ou aux tiers autorisés par les entreprises utilisatrices,* ***un accès et une utilisation*** *effectifs, de haute qualité, continus et en temps réel* ***pour les données agrégées ou non agrégées*** *fournies ou générées dans le cadre de l'utilisation des services de plateforme essentiels concernés par ces entreprises utilisatrices et par les utilisateurs finaux qui se servent des produits et services qu'elles fournissent; en ce qui concerne les* ***données à caractère personnel****, ne procure l'accès et l'utilisation que lorsqu'ils sont directement liés à l'utilisation faite par* ***l'utilisateur final*** *en lien avec les produits ou services que l'entreprise utilisatrice concernée fournit par l'intermédiaire du service de plateforme essentiel concerné,* ***et lorsque l'utilisateur final opte pour un tel partage de données en manifestant son consentement au sens du règlement (UE) 2016/679***».

31. Le CEPD estime que l'article 6, paragraphe 1, point i) tel qu'il est rédigé peut prêter à confusion, ce qui pourrait conduire à une incohérence avec le RGPD. Telle qu'elle est actuellement rédigée, la proposition pourrait être comprise en ce sens que les «données agrégées ou non agrégées» (mentionnées à la première phrase avant, et par opposition à la deuxième phrase commençant par «en ce qui concerne les données à caractère personnel») n'incluent **pas** les données à caractère personnel, alors que les données agrégées ou non agrégées peuvent inclure des données à caractère personnel.

    En outre, la référence «**au sens du règlement (UE) 2016/679**» pourrait être mieux précisée.

    Le CEPD recommande donc de préciser qu'un contrôleur d'accès procure gratuitement aux entreprises utilisatrices, ou aux tiers autorisés par les entreprises utilisatrices, un **accès et une utilisation** sans coût, effectifs, de haute qualité, continus et en temps réel pour les **données à caractère non personnel** fournies ou générées dans le cadre de l'utilisation des services de plateforme essentiels concernés par ces entreprises utilisatrices et par les utilisateurs finaux qui se servent des produits et services qu'elles fournissent; et qu'un contrôleur d'accès donne, **en pleine conformité avec le RGPD**, aux entreprises utilisatrices la possibilité d'obtenir le **consentement de la personne concernée**, autorisant les entreprises utilisatrices à utiliser les **données à caractère personnel** et à y accéder lorsqu'elles sont directement liées à l'utilisation faite par l'utilisateur final en lien avec les produits ou services que l'entreprise utilisatrice concernée fournit par l'intermédiaire du service de plateforme essentiel concerné. Le CEPD recommande également de préciser que les fonctionnalités permettant de fournir des informations et d'offrir la possibilité d'accorder un consentement devraient être **aussi conviviales que possible**.

32. **L'article 6, paragraphe 1, point j)** de la proposition dispose que le contrôleur d'accès «*procure à tout fournisseur tiers de 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 les moteurs de recherche en ligne du contrôleur d'accès,* ***sous réserve d'anonymisation pour les données de requêtes, de clics et de vues qui constituent des données à caractère personnel****;*»;

    À cet égard, le CEPD note que les **données concernant les requêtes, clics et vues** en lien avec les recherches générées par des personnes constituent des **données à caractère personnel**. En outre, ces données sont susceptibles d'être **de nature très sensible** car elles

peuvent contribuer à établir un profil des préférences, du statut (y compris l'état de santé), des intérêts et des convictions (y compris les convictions religieuses et politiques) de l'individu.

Le CEPD estime également que, dans la pratique, le responsable du traitement n'accorde souvent pas l'attention voulue à l'**anonymisation effective** des données à caractère personnel et que, par conséquent, le partage de ces informations entraîne un risque élevé de ré-identification. En effet, compte tenu du niveau élevé d'informations sur la vie privée des personnes concernées par les données concernant les requêtes, clics et vues, le CEPD estime que l'impact d'une ré-identification serait en général très élevé.

À la lumière de ce qui précède, le CEPD recommande de préciser dans un considérant que le contrôleur d'accès doit être en mesure de démontrer que les données anonymisées de requêtes, de clics et de vues **ont été testées de manière adéquate au regard des risques éventuels de ré-identification**.

33. Le CEPD se félicite de la précision, à **l'article 7, paragraphe 1,** de la proposition selon laquelle «*[l]es mesures que le contrôleur d'accès met en œuvre pour garantir le respect des obligations énoncées aux articles 5 et 6 atteignent de manière effective l'objectif de l'obligation pertinente. Le contrôleur d'accès veille à ce que ces mesures* ***soient mises en œuvre dans le respect du règlement (UE) 2016/679 et de la directive 2002/58/CE****, ainsi que de la législation relative à la cybersécurité, à la protection des consommateurs et à la sécurité des produits*».

34. En ce qui concerne l'**article 10** de la proposition, *Mise à jour des obligations des contrôleurs d'accès*, le CEPD recommande d'ajouter à l'**article 10, paragraphe 2, point a),** une référence aux **utilisateurs finaux**, en plus des entreprises utilisatrices, lorsqu'il est fait référence au déséquilibre des droits et des obligations avec le contrôleur d'accès et à l'avantage que le contrôleur d'accès obtiendrait. Cet ajout serait conforme aux objectifs généraux de la proposition et contribuerait à les soutenir, en vue de renforcer la contestabilité et l'équité des services de plateforme essentiels, compte tenu également du déséquilibre entre le contrôleur d'accès et l'utilisateur final.

35. **L'article 11, paragraphe 2,** de la proposition dispose que «*[s]i le consentement est requis pour la collecte et le traitement 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 desdites données, lorsqu'il est exigé par application du règlement (UE) 2016/679 et 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*».

    À cet égard et dans un souci de précision, le CEPD recommande de remplacer «soit» [pour se conformer aux] par «et».

36. **L'article 13**, Obligation d'audit, fournit un autre exemple clair de la forte **complémentarité** entre le droit de la concurrence et le droit relatif à la protection des données. En vertu de l'article 13, un contrôleur d'accès «*soumet à la Commission une* ***description, devant faire 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 recensés en application de l'article 3. Cette description est mise à jour au moins une fois par an*».

À cet égard, le CEPD considère que cette obligation peut présenter un intérêt pour réduire l'«avantage tiré des données» du contrôleur d'accès et, par ailleurs, réduire **l'asymétrie de l'information** entre ce dernier et les autorités de contrôle publiques (et, en dernier ressort, entre les contrôleurs d'accès et les personnes concernées) en ce qui concerne le traitement des données à caractère personnel. En outre, cet audit peut contribuer à détecter le profilage des consommateurs qui **n'est pas** proportionné ou qui n'est pas conforme au RGPD et aux droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel, tels qu'établis par les articles 7 et 8 de la charte des droits fondamentaux de l'Union européenne[28].

Compte tenu ce qui précède, le CEPD recommande que la proposition précise que la description, devant faire l'objet d'un audit, ainsi que tout document pertinent qui est collecté dans le cadre de la surveillance des contrôleurs d'accès en rapport avec le traitement des données à caractère personnel, est transmis par la Commission à toute autorité de contrôle compétente représentée au sein du comité européen de la protection des données, à sa demande.

3.5. Interopérabilité des plateformes

37. Le CEPD estime que les questions relatives au manque de contestabilité et aux possibilités d'entrée sur le marché que la proposition vise à examiner sont exacerbées par le caractère fermé des contrôleurs d'accès («walled gardens» ou écosystèmes fermés). **Une interopérabilité accrue** peut faciliter le développement d'un environnement numérique plus ouvert et pluraliste et créer de nouvelles possibilités de développement de services numériques innovants.

38. Le CEPD recommande au colégislateur d'envisager d'introduire des exigences minimales d'interopérabilité pour les contrôleurs d'accès, avec l'obligation explicite pour ces derniers de soutenir l'interopérabilité et de ne pas prendre de mesures qui l'entraveraient. Le CEPD suggère d'élaborer au niveau européen des **normes techniques d'interopérabilité** qui devraient être approuvées par les contrôleurs d'accès (dans ses différentes spécifications, à savoir l'interopérabilité des protocoles, l'interopérabilité des données, l'interopérabilité complète des protocoles[29]). Ces normes techniques devraient être conformes à la législation européenne en matière de protection des données, ne pas abaisser le niveau de sécurité offert par les plateformes et ne pas entraver l'innovation en raison de normes d'interopérabilité trop détaillées. Les organisations européennes de normalisation, en consultation, le cas échéant, avec le comité européen de la protection des données, devraient élaborer des normes qui satisfont à ces exigences. La Commission devrait avoir la possibilité de demander aux organisations européennes de normalisation d'élaborer de telles normes européennes, conformément à la législation de l'Union applicable en matière de normalisation européenne.[30]

3.6. Comité consultatif en matière de marchés numériques

39. En ce qui concerne le **comité consultatif en matière de marchés numériques**, institué en vertu de **l'article 32** de la proposition, le CEPD recommande de faire **explicitement référence** aux autorités dont le comité consultatif sera composé. Compte tenu de l'incidence de la proposition sur différents domaines du droit de l'Union, et notamment en raison des interactions avec **la protection des données à caractère personnel**, le CEPD recommande de préciser à l'article 32, paragraphe 1, que le comité consultatif en matière de marchés

numériques est composé de représentants du **comité européen de la protection des données institué conformément à l'article 68 du RGPD**, ainsi que de représentants des autorités compétentes des États membres en matière de concurrence, de communications électroniques, de services audiovisuels, de contrôle électoral et de protection des consommateurs.

40. Fort de l'expérience acquise en ce qui concerne la Digital Clearinghouse[31], le CEPD recommande vivement de mettre en place une **coopération institutionnalisée et structurée** entre les autorités de contrôle compétentes et, notamment, les autorités chargées de la protection des données. À cet égard, le CEPD considère que la Commission devrait consulter les autorités compétentes concernées, y compris les autorités chargées de la protection des données, dans le cadre de leurs enquêtes et évaluations (par exemple, sur la désignation d'un contrôleur d'accès); le CEPD fait dès lors valoir que la proposition devrait spécifiquement mentionner ce pouvoir de la Commission, dans un souci de sécurité juridique.

41. Le chapitre V de la proposition **devrait également établir une base juridique claire pour permettre l'échange de toute information pertinente entre les autorités compétentes** (par exemple, tout document pertinent qui est collecté dans le cadre de la surveillance des contrôleurs d'accès et qui concerne des aspects liés au traitement des données à caractère personnel). Cela impliquerait également une modification de l'article 31 de la proposition, qui limite explicitement l'utilisation des informations recueillies par application des articles 3, 12, 13, 19, 20 et 21 aux seules fins de la législation sur les marchés numériques. Cela permettrait de soutenir davantage les objectifs sous-jacents de la proposition en permettant à chaque autorité compétente de remplir ses rôles complémentaires, tout en agissant conformément à son mandat et à sa mission de service public respectifs.

4. CONCLUSIONS

À la lumière des considérations qui précèdent, le CEPD émet les recommandations suivantes:

- préciser que la proposition **complète** à la fois le règlement 2016/679 **et la directive 2002/58/CE**, et que la proposition **ne précise ni ne remplace** aucune des obligations des services de plateforme essentiels en vertu du règlement 2016/679 et de la directive 2002/58/CE;

- préciser à **l'article 5, point a)**, de la proposition que le contrôleur d'accès fournit aux utilisateurs finaux **une solution conviviale** (d'accessibilité facile et rapide) pour la **gestion du consentement**, conformément au règlement 2016/679, et en particulier l'exigence de respect de la vie privée dès la conception et de respect de la vie privée par défaut énoncée à l'article 25 du règlement 2016/679;

- ajouter une référence aux **utilisateurs finaux** à **l'article 5, point f), de la proposition**;

- préciser le champ d'application de la portabilité des données prévue à **l'article 6, paragraphe 1, point h)**, de la proposition;

- reformuler **l'article 6, paragraphe 1, point i),** de la proposition afin de garantir la conformité avec le RGPD, en tenant compte en particulier de la définition des «données à caractère personnel» figurant à l'article 4, paragraphe 1, du RGPD;

- renforcer la référence à **l'article 6, paragraphe 1, point j)**, de la proposition, en précisant dans un considérant que le contrôleur d'accès doit être en mesure de démontrer que les données anonymisées de requêtes, de clics et de vues ont été testées de manière adéquate au regard des risques éventuels de ré-identification;

- ajouter une référence aux **utilisateurs finaux à l'article 10, paragraphe 2, point a)**, de la proposition;

- reformuler **l'article 11, paragraphe 2**, de la proposition en remplaçant «ou» par «et»;

- préciser que **la description, devant faire l'objet d'un audit,** est communiquée par la Commission au comité européen de la protection des données ou, à tout le moins, aux autorités de contrôle compétentes en vertu du RGPD, à leur demande;

- préciser, à **l'article 32, paragraphe 1**, que le comité consultatif en matière de marchés numériques est composé de représentants du comité européen de la protection des données, ainsi que de représentants des autorités compétentes des États membres en matière de concurrence, de communications électroniques, de services audiovisuels, de contrôle électoral et de protection des consommateurs;

- envisager d'introduire des **exigences minimales d'interopérabilité** pour les contrôleurs d'accès et promouvoir l'élaboration de normes techniques au niveau européen, conformément à la législation de l'Union applicable en matière de normalisation européenne;

- mettre en place une **coopération institutionnalisée et structurée** entre les autorités de surveillance compétentes concernées, y compris les autorités chargées de la protection des données. Cette coopération devrait notamment permettre d'échanger toutes les informations pertinentes avec les autorités compétentes afin qu'elles puissent remplir leur rôle complémentaire, tout en agissant conformément à leur mandat institutionnel respectif.

Bruxelles, le 10 février 2021

Wojciech WIEWIÓROWSKI
(signature électronique)

NOTES

[1] JO L 119 du 4.5.2016, p. 1.

[2] JO L 201 du 31.7.2002, p. 37.

[3] JO L 295 du 21.11.2018, p. 39.

[4] COM(2020) 842 final.

[5] COM(2020) 67 final.

[6] COM(2020) 842 final, p. 1.

[7] COM(2020) 842 final, p. 2.

[8] https://edps.europa.eu/press-publications/press-news/press-releases/2020/shaping-safer-digital-future-new-strategy-new_de

[9] Exposé des motifs de la proposition, p. 2.

[10] Considérant 61 de la proposition.

[11] «A new pro-competition regime for digital markets Advice of the Digital Markets Taskforce» [un nouveau régime favorable à la concurrence pour les marchés numériques. Avis du groupe de travail sur les marchés numériques], 8 décembre 2020, disponible à l'adresse suivante:

https://assets.publishing.service.gov.uk/media/5fce7567e90e07562f98286c/Digital_Taskforce_-_Advice_--.pdf

[12] «Investigation of competition in digital markets» [enquête sur la concurrence sur les marchés numériques], Rapport et recommandations du personnel de la majorité, sous-commission sur le droit des ententes, le droit commercial et administratif, Commission Justice, États-Unis, 2020, disponible à l'adresse suivante:

https://judiciary.house.gov/uploadedfiles/competition_in_digital_markets.pdf

[13] Notamment, «Avis préliminaire du Contrôleur européen de la protection des données Vie privée et compétitivité à l'ère de la collecte de données massives: l'interaction entre le droit à la protection des données, le droit de la concurrence et la protection des consommateurs dans l'économie numérique», mars 2014, disponible à l'adresse:

https://edps.europa.eu/sites/edp/files/publication/14-03-26_competition_law_big_data_en.pdf

Avis nº 7/2015, «Relever les défis des données massives. Un appel à la transparence, au contrôle par l'utilisateur, à la protection des données dès la conception et à la reddition des comptes», disponible à l'adresse:

https://edps.europa.eu/sites/edp/files/publication/15-11-19_big_data_en.pdf

Avis nº 8/2016 du CEPD sur une application cohérente des droits fondamentaux à l'ère des données massives (Big Data), disponible à l'adresse:

https://edps.europa.eu/sites/edp/files/publication/16-09-23_bigdata_opinion_en.pdf

[14] Avis du CEPD sur une application cohérente des droits fondamentaux à l'ère des données massives (Big Data), 23 septembre 2016, disponible à l'adresse: https://edps.europa.eu/data-protection/our-work/publications/opinions/big-data_en

[15] Article de blog du CEPD «Carrying the torch in times of darkness» [porter le flambeau en période d'obscurité] 30 avril 2020, disponible à l'adresse suivante: https://edps.europa.eu/press-publications/press-news/blog/carrying-torch-times-darkness_en

[16] COM(2020) 842 final, p. 4.

[17] 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).

[18] Nous notons que l'article 1er, paragraphe 3, de la proposition **exclut** de son champ d'application les marchés liés aux **réseaux et services de communications électroniques**. L'une des particularités de la directive «vie privée et communications électroniques» réside toutefois dans le fait que deux de ses dispositions (l'article 5, paragraphe 3, et l'article 13) ont un **champ d'application plus large** que les autres dispositions, dont le champ d'application est limité

à la fourniture de services de communications électroniques accessibles au public sur les réseaux publics de communications. En conséquence, eu égard aux dispositions susmentionnées, la directive «vie privée et communications électroniques» s'applique aussi bien aux fournisseurs de services de communications électroniques **qu'aux opérateurs de sites internet (par exemple pour les cookies) ou à d'autres entreprises** (par exemple pour le marketing direct). Voir Comité européen de la protection des données, *«Avis 5/2019 relatif aux interactions entre la directive 'vie privée et communications électroniques' et le RGPD, en particulier en ce qui concerne la compétence, les missions et les pouvoirs des autorités de protection des données*, adopté le 12 mars 2019, notamment les paragraphes 23 et 28.

https://edpb.europa.eu/sites/edpb/files/files/file1/201905_edpb_opinion_eprivacydir_gdpr_interplay_en_0.pdf

Cela déclenche l'applicabilité de la directive «vie privée et communications électroniques» également dans le contexte de la proposition.

[19] Article 2, définition 20).

[20] Article 2, définition 21).

[21] Considérant 61; article 13 de la proposition; voir la définition de «profilage» à l'article 4, paragraphe 4, du RGPD.

[22] Considérants 55; 61; article 5, point a); article 6, paragraphe 1, point i); article 11, paragraphe 2, de la proposition; voir la définition de «consentement» à l'article 4, paragraphe 11 du RGPD.

[23] Article 6, paragraphe 1, point h), de la proposition; voir article 20 du RGPD pour le droit à la portabilité des données.

[24] Voir également considérant (2) de la proposition

[25] Dans les «Observations du CEPD sur la feuille de route pour l'évaluation de la communication de la Commission sur la définition du marché en cause aux fins du droit communautaire de la concurrence», le CEPD a fait observer ce qui suit: «*Comme l'ont fait observer les autorités de contrôle chargées de la protection des données, y compris le CEPD, dans la plupart des cas, les services numériques s'appuient sur le traitement de données à caractère personnel relatives aux utilisateurs (traitement étendu de données à caractère personnel, fourniture d'informations sur les préférences et les comportements des utilisateurs) en tant qu'élément essentiel - sinon le plus important - de leur modèle économique 'gratuit'.*

Le règlement (UE) 2016/679 (le «RGPD»), tel qu'interprété et appliqué par les autorités de contrôle, est donc un ***règlement d'interface essentiel*** *eu égard au droit et à la politique de la concurrence et, plus spécifiquement, aux questions relatives au* ***pouvoir de marché*** *et à la* ***définition du marché****. À cet égard, permettez-moi de souligner, entre autres, les principes relatifs au traitement des données à caractère personnel énoncés à l'article 5 du RGPD, au* ***droit à la portabilité des données*** *prévu à l'article 20 (visant, entre autres, à examiner la question de la captation de l'utilisateur) du RGPD, ainsi qu'aux dispositions du RGPD relatives au«****profilage****».*

*En ce qui concerne spécifiquement la communication de la Commission, nous tenons à souligner, à titre liminaire, que le «****pouvoir des données****» (pouvoir de marché découlant de la capacité de l'entreprise à traiter de grandes quantités et types de données à caractère personnel) est pertinent dans les deux cas suivants:*

(i) la substitution du côté de la ***demande****(par exemple, lorsque des données à caractère personnel provenant de différentes sources sont collectées et mises à la disposition de la même entreprise, par exemple une plateforme numérique - soit parce que la plupart des données de l'utilisateur se trouvent sur cette plateforme, et/ou parce que la plupart des personnes auxquelles l'utilisateur s'intéresse se trouvent sur cette plateforme - il est plus difficile pour l'utilisateur de* ***passer*** *à un autre fournisseur, ce qui est usuellement appelé la captation de l'utilisateur);*

(ii) la substitution du côté de ***l'offre****(l'intégration des données et des services basés sur ces données) peut rendre plus difficile, voire possible, la* ***fourniture de produits similaires par les concurrents*** *à court terme).*

Ces considérations, liées au traitement de données à caractère personnel, pourraient servir de base à l'évaluation, par la DG Concurrence, du ***pouvoir de marché*** *et de la possibilité* ***d'augmenter le prix*** *pour les consommateurs (également le* ***prix non monétaire****, dans un modèle freemium) après la fusion. Compte tenu de ce dernier aspect, nous soulignons qu'il existe un consensus croissant dans le monde universitaire sur la nécessité de considérer le «coût de la vie privée» ou l'«atteinte à la vie privée» (la possible dégradation du niveau de protection des données à caractère personnel) comme une dégradation du service, et donc comme un prix nonmonétaire».*

[26] Voir *Lignes directrices du comité européen de la protection des données sur le ciblage des utilisateurs des médias sociaux*, paragraphe 50: «[..] *Le groupe de travail «article 29» a précédemment estimé qu'il serait difficile pour les responsables du traitement de justifier le recours à des intérêts légitimes comme base légale pour des pratiques*

intrusives de profilage et de suivi à des fins de marketing ou de publicité, par exemple celles qui impliquent le suivi d'individus sur plusieurs sites web, emplacements, dispositifs, services ou courtage de données».

[27] Lignes directrices relatives au droit à la portabilité des données, adoptées le 13 décembre 2016, révisées et adoptées le 5 avril 2017, disponibles à l'adresse suivante: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611233

Voir plus particulièrement page 9, «Les catégories suivantes peuvent être qualifiées de données '**fournies par la personne concernée'**: - **les données activement et sciemment fournies par la personne concernée** (par exemple, adresse postale, nom d'utilisateur, âge, etc.) **- les données observées fournies par la personne concernée grâce à l'utilisation du service ou du dispositif.** Ces données peuvent inclure, par exemple, l'historique de recherche, les données relatives au trafic et les données de localisation d'une personne. Elles peuvent aussi inclure d'autres données brutes comme le rythme cardiaque enregistré par un dispositif portable. En revanche, les données déduites et les données dérivées sont créées par le responsable du traitement sur la base des données «fournies par la personne concernée». Par exemple, le résultat d'une appréciation relative à la santé d'un utilisateur ou un profil créé dans le contexte des réglementations relatives à la gestion des risques et de la réglementation financière (par ex., pour attribuer une cote de solvabilité ou respecter les règles en matière de lutte contre le blanchiment d'argent) ne peuvent pas être considérés en soi comme ayant été 'fournis' par la personne concernée».

[28] Considérant 61: «Garantir un niveau adéquat de transparence en ce qui concerne les pratiques de profilage utilisées par les contrôleurs d'accès permet de faciliter la contestabilité des services de plateforme essentiels, en exerçant une pression extérieure sur les contrôleurs d'accès afin d'éviter que le profilage approfondi du consommateur ne devienne la norme dans le secteur [...]».

[29] Voir également J. Crémer, Y.-A. de Montjoye et H. Schweitzer, «Competition Policy for the digital era», 2019, p. 58 et suivantes, à l'adresse suivante: https://ec.europa.eu/competition/publications/reports/kd0419345enn.pdf. Voir aussi avis du CEPD concernant la législation sur les services numériques.

[30] La Commission européenne devrait le demander aux organisations européennes de normalisation, conformément au règlement (UE) 1025/2012 du Parlement européen et du Conseil du 25 octobre 2012 relatif à la normalisation européenne, modifiant les directives 89/686/CEE et 93/15/CEE du Conseil et les directives 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE et 2009/105/CE du Parlement européen et du Conseil et abrogeant la décision 87/95/CEE du Conseil et la décision nº 1673/2006/CE du Parlement européen et du Conseil. *JO L 316 du 14.11.2012, p. 12-33.*

[31] Voir à l'adresse https://www.digitalclearinghouse.org/. La Digital Clearinghouse sert de forum de discussion entre les autorités chargées de la protection des données, de la protection des consommateurs et de la concurrence, ce qui a contribué à déplacer l'analyse de l'interaction entre les trois domaines politiques du niveau plus académique vers le contexte de l'élaboration des politiques et de la réglementation. La Digital Clearinghouse a été mise en place par le CEPD en 2016 avec l'avis sur une application cohérente des droits fondamentaux à l'ère des données massives (Big Data), 23 septembre 2016, plus d'informations sont disponibles à l'adressehttps://edps.europa.eu/data-protection/our-work/subjects/big-data-digital-clearinghouse_en