



EUROPEAN DATA PROTECTION SUPERVISOR

Avis n° 01/2021

**concernant la  
proposition de  
législation sur les  
services numériques**



10 février 2021

*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 Wiewiorowski 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 à un marché intérieur des services numériques (législation sur les services numériques) et modifiant la directive 2000/31/CE, adoptée par la Commission européenne.*

## Synthèse

Le 15 décembre 2020, la Commission a 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 (la «LSN»).

Le CEPD salue l'objectif de la Commission, qui vise à promouvoir **un environnement en ligne transparent et sûr**, en définissant les responsabilités et l'obligation de rendre des comptes incombant aux services intermédiaires, et en particulier aux plateformes en ligne, telles que les médias sociaux et les places de marché.

Le CEPD se félicite que la proposition **visse à compléter plutôt qu'à remplacer les protections existantes en vertu du règlement (UE) 2016/679 et de la directive 2002/58/CE**. Cela étant dit, la proposition aura clairement une incidence sur le traitement des données à caractère personnel. Le CEPD estime qu'il est **nécessaire de garantir la complémentarité dans le contrôle et la surveillance** des plateformes en ligne et des autres fournisseurs de services d'hébergement.

Certaines activités réalisées dans le contexte des plateformes en ligne présentent des risques accrus non seulement pour les droits des individus, mais aussi pour la société dans son ensemble. Si la proposition comprend un ensemble de mesures d'atténuation des risques, des **garanties supplémentaires** sont nécessaires, notamment en ce qui concerne **la modération des contenus, la publicité en ligne et les systèmes de recommandation**.

La modération des contenus devrait se faire dans le respect de **l'État de droit**. Eu égard à la **surveillance déjà caractéristique** du comportement des individus, en particulier dans le contexte des plateformes en ligne, la LSN devrait déterminer dans quels cas les efforts de lutte contre les «contenus illicites» légitiment l'utilisation de moyens automatisés pour détecter, recenser et combattre les contenus illicites. Le profilage à des fins de modération de contenu devrait être **interdit**, à moins que le fournisseur ne puisse démontrer que de telles mesures sont *strictement* nécessaires pour faire face aux risques systémiques explicitement déterminés par la LSN.

Compte tenu de la multitude de risques associés à la **publicité ciblée en ligne**, le CEPD exhorte les colégislateurs à envisager des **règles supplémentaires allant au-delà de la transparence**. Ces mesures devraient comprendre une **suppression progressive débouchant sur une interdiction de la publicité ciblée reposant sur un suivi omniprésent**, ainsi que des **restrictions** en ce qui concerne les catégories de données pouvant être traitées à des fins de ciblage et les catégories de données susceptibles d'être divulguées aux annonceurs ou à des tiers afin de permettre ou de faciliter la publicité ciblée.

Conformément aux exigences en matière de protection des données dès la conception et par défaut, **les systèmes de recommandation** ne devraient pas reposer, par défaut, sur le profilage. Eu égard à leur incidence significative, le CEPD recommande également de prendre des mesures supplémentaires visant à **promouvoir davantage la transparence et le contrôle des utilisateurs** en ce qui concerne les systèmes de recommandation.

Plus généralement, le CEPD recommande d'introduire des **exigences minimales d'interopérabilité** pour les très grandes plateformes en ligne et de promouvoir l'élaboration de normes techniques au niveau européen, conformément à la législation de l'Union applicable en matière de normalisation européenne.

Compte tenu de l'expérience et des évolutions liées à la **Digital Clearinghouse**, le CEPD recommande vivement de prévoir une base juridique explicite et complète pour **la coopération et l'échange d'informations pertinentes** entre les autorités de contrôle, agissant chacune dans leurs domaines de compétence respectifs. La législation sur les services numériques devrait garantir une **coopération institutionnalisée et structurée** entre les autorités compétentes en matière de surveillance, y compris les autorités chargées de la protection des données, les autorités de protection des consommateurs et les autorités de la concurrence.

## TABLE DES MATIÈRES

<b>1. INTRODUCTION .....</b>	<b>6</b>
<b>2. OBSERVATIONS GÉNÉRALES .....</b>	<b>7</b>
<b>3. RECOMMANDATIONS SPÉCIFIQUES .....</b>	<b>10</b>
3.1 LIEN AVEC LE RÈGLEMENT (UE) 2016/679 ET LA DIRECTIVE 2002/58/CE .....	10
3.2 «CONTENU ILLICITE» ET ABSENCE D'OBLIGATIONS GÉNÉRALES EN MATIÈRE DE SURVEILLANCE .....	10
3.3 INFORMATIONS RELATIVES À LA MODÉRATION DE CONTENU .....	12
3.4 NOTIFICATION ET ACTION ET L'OBLIGATION DE MOTIVATION .....	13
3.5 TRAITEMENT DES RÉCLAMATIONS .....	15
3.6 GARANTIES SUPPLÉMENTAIRES POUR LA MODÉRATION DE CONTENU .....	15
3.7 NOTIFICATION DE SOUPÇONS D'INFRACTIONS PÉNALES .....	17
3.8 TRANSPARENCE DE LA PUBLICITÉ EN LIGNE .....	18
3.9 SYSTÈMES DE RECOMMANDATION .....	19
3.10 ACCÈS DES CHERCHEURS AGRÉÉS .....	21
3.11 INTEROPÉRABILITÉ DES PLATEFORMES .....	22
3.12 MISE EN ŒUVRE, COOPÉRATION, SANCTIONS ET EXÉCUTION .....	22
<b>4. CONCLUSIONS .....</b>	<b>24</b>
<b>Notes .....</b>	<b>29</b>

## 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 ou RGPD)<sup>1</sup>,

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<sup>2</sup>, et notamment son article 42, paragraphe 1,

### A ADOPTÉ LE PRÉSENT AVIS:

## 1. INTRODUCTION

1. Le 15 décembre 2020, la Commission a 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<sup>3</sup>.
2. La proposition fait suite à la communication intitulée *Façonner l'avenir numérique de l'Europe*, dans laquelle la Commission a confirmé son intention d'élaborer des règles nouvelles et modifiées pour approfondir le marché intérieur des services numériques, en augmentant et en harmonisant les responsabilités des plateformes en ligne et des fournisseurs de services d'information et en renforçant le contrôle exercé sur les politiques des plateformes en matière de contenus dans l'UE<sup>4</sup>.
3. Selon l'exposé des motifs, des services numériques, nouveaux et innovants, ont profondément contribué aux transformations sociétales et économiques dans l'Union et dans le monde entier. Dans le même temps, l'utilisation de ces services est également devenue la source de risques et de défis nouveaux, tant pour la société dans son ensemble que pour les particuliers qui y ont recours<sup>5</sup>.
4. La proposition vise à garantir les meilleures conditions pour la fourniture de **services numériques innovants** dans le marché intérieur, à contribuer à la **sécurité en ligne** et à la protection des **droits fondamentaux**, ainsi qu'à mettre en place une **structure de gouvernance** solide et durable pour surveiller efficacement les fournisseurs de services intermédiaires<sup>6</sup>. À cette fin, la proposition:
  - renferme des dispositions relatives à l'exemption de responsabilité des prestataires de services intermédiaires (chapitre II);
  - impose des «obligations de diligence raisonnable», adaptées au type et à la nature du service intermédiaire concerné (chapitre III); et
  - contient des dispositions relatives à la mise en œuvre et à l'exécution de la proposition de règlement (chapitre IV).

5. Le CEPD a été consulté de manière informelle sur le projet de proposition de législation sur les services numériques le 27 novembre 2020. Le CEPD se félicite d’avoir été consulté à ce stade précoce de la procédure.
6. Outre la proposition de législation sur les services numériques, la Commission a également adopté 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)<sup>7</sup>. Conformément à l’article 42, paragraphe 1, du règlement (UE) 2018/1725, le CEPD a également été consulté sur la proposition de législation sur les marchés 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 notre société<sup>8</sup>.
8. Le CEPD soutient l’objectif de la Commission qui vise à promouvoir un **environnement en ligne transparent et sûr**, en définissant les responsabilités et l’obligation de rendre des comptes incombant aux services intermédiaires, et en particulier aux plateformes en ligne, telles que les médias sociaux et les places de marché.
9. Le CEPD se félicite de la reconnaissance du fait que certaines activités en ligne, en particulier dans le contexte des plateformes en ligne, présentent des risques croissants **non seulement pour les droits fondamentaux des individus, mais aussi pour la société dans son ensemble**<sup>9</sup>. Cela est d’autant plus évident pour les fournisseurs de très grandes plateformes en ligne et transparaît dans la considération selon laquelle les fournisseurs de très grandes plateformes devraient être soumis aux normes les plus strictes en matière de diligence raisonnable, proportionnellement à leur effet sociétal<sup>10</sup>.
10. Dans son avis sur la manipulation en ligne et les données à caractère personnel, le CEPD a recensé plusieurs risques et préjudices résultant de **la manière dont les données à caractère personnel sont utilisées pour déterminer l’expérience en ligne**<sup>11</sup>. L’avis soulignait également comment les modèles d’entreprise existants à l’origine de nombreux services en ligne ont contribué à accentuer la **polarisation politique et idéologique, la désinformation et la manipulation**. Des risques similaires ont également été mis en évidence par le comité européen de la protection des données (EDPB) dans ses lignes directrices relatives au ciblage des utilisateurs de médias sociaux<sup>12</sup>.
11. Le CEPD se félicite que la proposition reconnaisse que la **conception des services numériques** fournis par de très grandes plateformes en ligne est généralement optimisée au bénéfice de leurs **modèles économiques souvent axés sur la publicité** et peut **susciter des préoccupations sociétales**<sup>13</sup>. La proposition reconnaît également les éventuels préjudices causés par l’utilisation de **systèmes algorithmiques**, notamment en ce qui concerne leur potentiel d’**amplification** de certains contenus, y compris la désinformation<sup>14</sup>. Le CEPD considère que les phénomènes et les préjudices sont intrinsèquement liés à ce qu’il convient d’appeler l’«**économie de l’attention**», les services et les applications étant conçus de manière à maximiser l’attention et l’engagement afin de

recueillir davantage de données sur les clients, de mieux cibler la publicité et d'augmenter les revenus<sup>15</sup>.

12. Si la proposition comprend un ensemble de mesures d'atténuation des risques, la plupart des dispositions visent à promouvoir la **transparence et la responsabilité, sans s'attaquer directement à la cause profonde** au moyen de règles ex ante. Pour être clair, le CEPD soutient sans réserve les mesures visant à renforcer la transparence et la responsabilité des plateformes. Par ailleurs, **il convient de prendre des mesures supplémentaires** pour tenir dûment compte des risques systémiques mis en évidence ci-dessus, en particulier en ce qui concerne les très grandes plateformes en ligne. À cet égard, la proposition doit également être considérée à la lumière de la proposition de législation sur les marchés numériques, qui comprend des règles supplémentaires visant à promouvoir des marchés équitables et ouverts et le traitement équitable des données à caractère personnel<sup>16</sup>. Dans le présent avis, le CEPD recommandera également d'autres mesures à cet égard, y compris en ce qui concerne la publicité en ligne.
13. Le CEPD se félicite que la proposition vise à compléter plutôt qu'à remplacer les protections existantes en vertu du règlement (UE) 2016/679 et de la directive 2002/58/CE. Par exemple, les mesures concernant la publicité sur les plateformes en ligne complètent mais ne modifient pas les règles existantes sur le consentement et le droit d'opposition au traitement des données à caractère personnel<sup>17</sup>. Ce faisant, la proposition favorise la **complémentarité** (par opposition à l'ingérence) avec la **législation de l'Union en vigueur en matière de protection des données**. Cela étant dit, le CEPD estime également que certaines dispositions et mesures éventuelles **auront clairement une incidence** sur le traitement des données à caractère personnel et qu'il est donc nécessaire d'assurer la **complémentarité dans la surveillance et le contrôle** des plateformes en ligne et des autres fournisseurs de services d'hébergement.
14. Le CEPD fait observer que les obligations proposées incombant aux plateformes peuvent, dans la pratique, **accroître le recours aux plateformes pour préserver les valeurs publiques**. Les plateformes doivent, à juste titre, être tenues pour responsables du préjudice sociétal résultant des activités qu'elles contrôlent. Il convient également que les plateformes endossent la responsabilité des contenus encourageant les abus envers les enfants et d'autres groupes vulnérables<sup>18</sup>. Par ailleurs, des garanties appropriées devraient être introduites pour faire en sorte que les mesures visant à atténuer le préjudice soient prises **dans le respect de l'État de droit** et qu'elles n'entravent pas de manière disproportionnée les droits et libertés d'autrui.
15. Le CEPD rappelle que le droit à la protection des données n'est pas un **droit absolu** et que des ingérences peuvent être justifiées, à condition que ces mesures restent limitées à ce qui est nécessaire et proportionné. En outre, il n'y a pas de **conflit intrinsèque** entre le droit à la protection des données et les objectifs de la proposition visant à garantir un environnement en ligne innovant, transparent et sûr. **La protection des données et le respect de la vie privée font partie intégrante d'une économie numérique dynamique, y compris les plateformes en ligne**. La protection des données et le respect de la vie privée sont nécessaires pour permettre aux personnes de s'exprimer librement, d'accéder librement aux informations et d'être créatives<sup>19</sup>. La sécurité en ligne et les mécanismes visant à garantir la responsabilité des plateformes en ligne peuvent favoriser davantage la jouissance effective des droits fondamentaux.



16. Dans les paragraphes qui suivent, le CEPD formule des recommandations spécifiques visant à s'assurer que la proposition **complète efficacement le règlement (UE) 2016/679** et renforce la protection des libertés et droits fondamentaux des personnes concernées.

### 3. RECOMMANDATIONS SPÉCIFIQUES

#### 3.1 Lien avec le règlement (UE) 2016/679 et la directive 2002/58/CE

17. L'article 1<sup>er</sup>, paragraphe 5, point i), de la proposition dispose que la législation sur les services numériques s'entend «**sans préjudice**» des règles établies par 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. Le considérant (10) de la proposition précise en outre que «*[l]a 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*».
18. Le CEPD **se félicite** que la proposition ne vise pas à affecter l'application de la législation de l'Union en vigueur régissant le traitement des données à caractère personnel, y compris les missions et les pouvoirs des autorités de contrôle compétentes pour contrôler le respect de ces instruments.
19. Toutefois, dans un souci de sécurité juridique, le CEPD recommande d'**aligner** le libellé de l'article 1<sup>er</sup>, paragraphe 5, point i), de la proposition sur celui de l'**article 1<sup>er</sup>, paragraphe 5, point b), de la directive 2000/31/CE** (directive sur le commerce électronique)<sup>20</sup>. Cela permettrait de maintenir la cohérence avec la jurisprudence existante de la Cour de justice de l'Union européenne. Dans l'arrêt *La Quadrature du Net*, par exemple, la Cour a explicitement fait référence à l'article 1<sup>er</sup>, paragraphe 5, point b), de la directive sur le commerce électronique pour confirmer que cette directive ne peut en tout état de cause pas porter atteinte aux exigences résultant de la directive 2002/58/CE et du règlement (UE) 2016/679<sup>21</sup>.
20. En ce qui concerne la question de la responsabilité, la proposition maintient les **règles en matière de responsabilité des fournisseurs de services intermédiaires** énoncées dans la directive sur le commerce électronique, tout en tenant compte des précisions apportées par la jurisprudence de la Cour de justice de l'Union européenne. Le considérant (17) dispose que «*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*»<sup>22</sup>. Le CEPD rappelle que le règlement (UE) 2016/679 contient des règles spécifiques qui régissent la responsabilité des responsables du traitement et des sous-traitants<sup>23</sup>. Dans un souci de sécurité juridique, le CEPD recommande de préciser que la proposition ne s'applique pas aux questions relatives aux services de la société de l'information qui sont couvertes par le règlement (UE) 2016/679 et la directive 2002/58/CE, y compris la responsabilité des responsables du traitement et des sous-traitants.

#### 3.2 «Contenu illicite» et absence d'obligations générales en matière de surveillance

21. En vertu de l'article 2, point g), on entend par «contenu illicite» «*toute information qui, en soi ou de par sa référence à une activité, [...] n'est pas conforme au droit de l'Union ou au droit d'un État membre, quel qu'en soit l'objet précis ou la nature précise*».
22. Le considérant (12) précise que la **notion de contenu illicite** doit faire l'objet d'une **définition large**, recouvrant les informations «relatives» aux contenus, produits, services

et activités illicites. Les exemples cités comprennent les discours de haine illégaux, les contenus à caractère terroriste, les contenus discriminatoires illégaux, le partage d'images représentant des abus sexuels commis sur des enfants, le partage illégal d'images privées sans consentement, le harcèlement en ligne, la vente de produits non conformes ou contrefaits, l'utilisation non autorisée de matériel protégé par le droit d'auteur ou les activités impliquant des infractions à la loi sur la protection des consommateurs. Le considérant (12) indique également que la législation nationale définissant l'illégalité devrait être «conforme au droit de l'Union». Dans un souci de sécurité juridique, le CEPD recommande de faire référence à l'article 52 de la Charte des droits fondamentaux de l'Union européenne, qui fixe les conditions de toute limitation de l'exercice des droits et libertés reconnus par la charte.

23. Le CEPD note que la proposition **n'impose pas une obligation générale de surveillance ou une obligation de recherche active des faits**, ni une obligation générale, pour les fournisseurs, de prendre des mesures proactives à l'égard des contenus illicites<sup>24</sup>. L'article 7 **interdit** en réalité d'imposer de telles obligations, sans préjudice d'éventuelles injonctions d'agir contre un élément de contenu illicite spécifique, émises par les autorités nationales ou judiciaires compétentes conformément à l'article 8.
24. La proposition **visé toutefois à éliminer les facteurs qui dissuadent actuellement** les fournisseurs de services intermédiaires **de mener volontairement leurs propres enquêtes** (article 6)<sup>25</sup>. En outre, plusieurs dispositions précisent que, dans la pratique, les efforts visant à recenser, détecter ou retirer des contenus illicites peuvent impliquer le traitement de données à caractère personnel, en particulier lors de l'utilisation de moyens automatisés.
25. Le CEPD souligne que toutes les formes de modération de contenu ne nécessitent pas l'attribution à une personne concernée spécifique. Conformément aux exigences de **minimisation des données et de protection des données dès la conception et par défaut**, la modération de contenu ne devrait, dans la mesure du possible, impliquer aucun traitement de données à caractère personnel. Le CEPD encourage le colégislateur à inclure un considérant à cet effet. Lorsque le traitement de données à caractère personnel est nécessaire, par exemple pour le mécanisme de réclamation, ces données ne devraient concerner que celles nécessaires à cette finalité spécifique, tout en appliquant l'ensemble des autres principes du règlement (UE) 2016/679<sup>26</sup>.
26. Dans un souci de sécurité juridique pour toutes les parties concernées, le CEPD recommande de **préciser dans quelles circonstances les efforts de lutte contre les «contenus illicites» légitiment le traitement de données à caractère personnel**, en particulier lorsqu'ils peuvent impliquer des moyens automatisés pour «détecter, recenser et combattre» les contenus illicites, qu'ils soient ou non effectués
  - sur une base volontaire ou obligatoire;
  - sur la base de notifications ou d'enquêtes d'initiative propre; ou
  - dans le contexte de la prise en considération des «risques systémiques» visés aux articles 26 et 27.

La proposition devrait également préciser si, et le cas échéant, dans quelle mesure, les fournisseurs de services intermédiaires sont **autorisés à notifier volontairement** aux services répressifs ou judiciaires des soupçons d'infractions pénales (par exemple, dans le

cadre d'informations permettant de soupçonner qu'une infraction pénale autre que celles prévues à l'article 21 est susceptible d'avoir été commise).

27. Le CEPD rappelle que même des mesures volontaires peuvent constituer une atteinte aux droits à la protection des données et à la vie privée<sup>27</sup>. En l'absence de garanties supplémentaires, la proposition risque de contribuer indirectement au traitement de données à caractère personnel qui n'est pas proportionné aux objectifs poursuivis, notamment en ne précisant pas les types de contenus illicites qui peuvent effectivement justifier l'utilisation de techniques de détection automatisées impliquant le traitement de données à caractère personnel, ou en ne définissant pas les circonstances dans lesquelles une notification volontaire peut avoir lieu. Des recommandations supplémentaires concernant des garanties relatives à l'utilisation de moyens automatisés impliquant le traitement de données à caractère personnel pour détecter, repérer et combattre les contenus illicites sont formulées ultérieurement dans le présent avis (section 3.6).

### 3.3 Informations relatives à la modération de contenu

28. Le chapitre III de la proposition définit les obligations de diligence pour un environnement en ligne sûr et transparent, adaptées au type et à la nature du service intermédiaire concerné<sup>28</sup>.
29. La première série d'obligations s'applique à tous les fournisseurs de services intermédiaires, y compris l'obligation d'indiquer dans leurs **conditions générales** les éventuelles restrictions qu'ils imposent en ce qui concerne l'utilisation de leurs services. Chaque fournisseur doit également agir de manière responsable dans l'application et le **contrôle de l'application** de ces restrictions.
30. En vertu de l'article 12, paragraphe 1, les renseignements à fournir incluent 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. Ils sont énoncés clairement et sans ambiguïté et sont publiquement disponibles dans un format facilement accessible»*.
31. La «modération des contenus» fait référence aux activités entreprises par les fournisseurs de services intermédiaires destinées à *«détecter et à repérer les contenus illicites ou les informations incompatibles avec leurs conditions générales et à lutter contre ces contenus ou informations»*. Ces activités comprennent les mesures prises qui ont une incidence sur la disponibilité, la visibilité et l'accessibilité de ces contenus ou informations, telles que leur *rétrogradation*, leur retrait ou *le fait de les rendre inaccessibles*, ou sur la capacité du bénéficiaire à fournir ces informations, telles que *la suppression ou la suspension* du compte d'un utilisateur<sup>29</sup>.
32. La définition de la modération des contenus indique clairement qu'elle **peut** - mais ne doit pas nécessairement - **impliquer le traitement de données à caractère personnel** d'une manière qui porte atteinte aux droits et intérêts des personnes concernées. Le CEPD tient à souligner qu'en fonction des catégories de données traitées et de la nature du traitement, la modération automatisée des contenus peut avoir une incidence significative à la fois sur le droit à **la liberté d'expression** et sur le **droit à la protection des données**.

33. Le CEPD croit comprendre que l'obligation de fournir des renseignements prévue à l'article 12, paragraphe 1, de la proposition est **complémentaire et sans préjudice** de l'obligation des fournisseurs de communiquer des informations aux personnes concernées conformément aux articles 12 à 14 du règlement (UE) 2016/679<sup>30</sup>. Le CEPD se félicite de cette disposition dans la mesure où elle vise à **accroître davantage encore la transparence** des pratiques de modération des contenus, y compris celles impliquant le traitement de données à caractère personnel.
34. Dans le même ordre d'idées, le CEPD se félicite également de l'article 13 de la proposition, qui **instaure des obligations en matière de rapports de transparence** imposant la publication, au moins une fois par an, de rapports sur les éventuelles activités de modération du contenu auxquelles les fournisseurs de services intermédiaires se sont livrés au cours de la période concernée. En ce qui concerne les plateformes en ligne, l'obligation est utilement complétée par l'article 23, paragraphe 1, point c), qui dispose que le rapport doit également intégrer, notamment, des informations relatives à *«tout recours à des moyens automatisés à des fins de modération de contenus, y compris une spécification des objectifs précis, des indicateurs de la précision des moyens automatisés pour atteindre ces objectifs et des éventuelles mesures de sauvegarde appliquées»*. S'agissant des très grandes plateformes en ligne, l'article 33 exige en outre la publication (sous réserve d'une éventuelle modification) des résultats de l'évaluation des risques, des mesures d'atténuation des risques et des rapports d'audit (de mise en œuvre) conformément aux articles 26 à 28 de la proposition. Le CEPD **soutient fermement** les articles 26 à 28 et 33 de la proposition, et en particulier l'obligation faite aux très grandes plateformes en ligne de se soumettre à des audits externes et indépendants et de **publier les rapports d'audit et d'évaluation des risques y afférents**.
35. L'incidence potentielle de la modération des contenus sur les droits fondamentaux est confirmée par l'article 12, paragraphe 2, de la proposition, qui prévoit que *«[l]orsqu'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 concernées, et notamment des **droits fondamentaux applicables des bénéficiaires du service, tels que consacrés dans la Charte**»*.
36. L'incidence potentielle sur les droits fondamentaux **peut varier considérablement** selon les moyens utilisés ainsi que leurs conséquences, qui peuvent aller de la rétrogradation du contenu à la suppression du compte d'un utilisateur, en passant par la notification éventuelle aux services répressifs de soupçons d'infractions pénales<sup>31</sup>.
37. Le CEPD se félicite que la proposition prévoit d'importantes garanties pour réduire au minimum l'effet potentiellement préjudiciable sur les droits fondamentaux, mais il recommande de **renforcer les dispositions pertinentes du point de vue de la protection** des données, en particulier dans les situations impliquant le **profilage** ou la **prise de décision automatisée**, comme décrit plus loin dans le présent avis<sup>32</sup>.

### 3.4 Notification et action et l'obligation de motivation

38. Les articles 14 et 15 contiennent des dispositions supplémentaires applicables aux fournisseurs de services d'hébergement, y compris les plateformes en ligne (qui stockent

non seulement les informations à la demande du bénéficiaire du service, mais diffusent également ces informations au public<sup>33</sup>).

39. Les fournisseurs de services d'hébergement établissent des mécanismes permettant à tout individu ou à toute entité de leur signaler la présence au sein de leur service d'informations spécifiques considérées comme du contenu illicite par l'individu ou l'entité<sup>34</sup>. Ces notifications doivent être suffisamment précises et motivées pour permettre à un opérateur économique diligent d'établir l'illégalité du contenu en question<sup>35</sup>.
40. En vertu de l'article 14, paragraphe 6, les fournisseurs de services d'hébergement peuvent faire appel à des **moyens automatisés aux fins du traitement ou de la prise de décisions** concernant les notifications reçues (auquel cas ils doivent communiquer à l'individu ou à l'entité ayant soumis la notification des informations sur cette utilisation, à condition que la notification mentionne le nom et une adresse de courrier électronique de l'individu l'ayant soumise)<sup>36</sup>.
41. L'article 15 exige du fournisseur de services d'hébergement de **fournir un exposé clair et spécifique des motifs** de toute décision de retirer des informations spécifiques fournies par les bénéficiaires du service ou d'empêcher l'accès à celles-ci, **indépendamment des moyens utilisés pour détecter, repérer ou retirer ces informations, ou empêcher l'accès** à celles-ci.
42. Le CEPD rappelle que **l'article 22 du règlement (UE) 2016/679** impose des conditions strictes pour les décisions fondées exclusivement sur un traitement automatisé, y compris le profilage, conduisant à des décisions susceptibles de produire des effets juridiques, ou d'affecter la personne concernée de manière significative de façon similaire. En outre, même en l'absence de prise de décision exclusivement automatisée, tout profilage est susceptible de présenter des risques importants pour les droits et les libertés des personnes concernées<sup>37</sup>.
43. Le CEPD se félicite de l'obligation, pour les fournisseurs de services d'hébergement, de fournir «*le cas échéant, des informations relatives à l'utilisation de moyens automatisés pour prendre la décision, y compris lorsque cette dernière concerne des contenus détectés ou repérés par des moyens automatisés*»<sup>38</sup>. Il importe de noter que cette exigence s'applique dans les situations où les décisions ne sont pas uniquement prises par des moyens automatisés et/ou n'impliquent pas de profilage. Pour accroître davantage encore la transparence, le CEPD recommande de modifier l'article 15, paragraphe 2, pour indiquer sans ambiguïté que **des informations relatives à l'utilisation de moyens automatisés pour détecter et repérer des contenus illicites doivent en tout état de cause être fournies**, indépendamment de la question de savoir si la décision prise ultérieurement impliquait l'utilisation de moyens automatisés ou non<sup>39</sup>.
44. Afin de garantir une véritable transparence, le CEPD recommande de renforcer les **exigences de transparence** énoncées à l'article 14, paragraphe 6, et à l'article 15, paragraphe 2, point c), en précisant davantage les informations à fournir aux personnes concernées lorsqu'elles sont informées de la décision en question. Le CEPD estime que les plateformes en ligne utilisant des moyens automatisés pour la modération de contenu ou la prise de décision devraient au moins informer les personnes concernées de la procédure suivie, de la technologie utilisée et des critères et motifs qui sous-tendent la décision, sans

préjudice de l'obligation d'information et des droits des personnes concernées en vertu du règlement (UE) 2016/679.

45. Le CEPD **se félicite**, à titre de garantie supplémentaire, de l'obligation faite aux fournisseurs de services d'hébergement de publier leurs décisions et les exposés des motifs dans une **base de données accessible au public** gérée par la Commission, avec l'exigence explicite que ces informations ne contiennent pas de données à caractère personnel<sup>40</sup>.

### 3.5 Traitement des réclamations

46. En vertu de l'article 17, les plateformes en ligne sont tenues de prévoir un système **interne de traitement des réclamations**, permettant d'introduire des réclamations contre les décisions de la plateforme de retirer les informations ou de rendre l'accès à celles-ci impossible ou de suspendre ou résilier la fourniture du service (ou le compte). L'article 17, paragraphe 5, prévoit que les plateformes doivent veiller à ce que les décisions concernant ces réclamations **ne soient pas uniquement prises par des moyens automatisés**.
47. Le CEPD est favorable à l'article 17 de la proposition; il recommande cependant d'introduire une garantie similaire concernant **tous les fournisseurs de services d'hébergement**, et pas seulement les plateformes en ligne, lorsque la détection et le repérage de contenus illicites impliquent le traitement de données à caractère personnel. En effet, la proposition elle-même fait allusion au fait que tout fournisseur de services d'hébergement peut potentiellement utiliser des moyens automatisés pour la détection, le repérage et les décisions éventuelles concernant les contenus illicites<sup>41</sup>. Lorsque ces mécanismes impliquent le traitement de données à caractère personnel, les personnes devraient disposer d'un mécanisme de réclamation facilement accessible, comme le prévoit l'article 17, indépendamment du fait que le fournisseur du service d'hébergement diffuse ou non des informations au public.
48. Enfin, le CEPD recommande aussi d'insérer à l'article 17 **un délai** dans lequel la plateforme doit rendre la décision relative à la réclamation, ainsi que l'indication selon laquelle le mécanisme de réclamation qui doit être mis en place est sans préjudice des droits et voies de recours dont disposent les personnes concernées conformément au règlement (UE) 2016/679 et à la directive 2002/58/CE<sup>42</sup>.

### 3.6 Garanties supplémentaires pour la modération de contenu

49. Comme indiqué ci-dessus, le CEPD se félicite que la proposition comprenne plusieurs garanties visant à réduire au minimum le risque d'atteinte injustifiée aux droits fondamentaux, notamment en prévoyant une obligation d'information, une obligation de motivation et une obligation de mettre en place un mécanisme interne de traitement des réclamations qui ne statuera pas uniquement par le biais de moyens automatisés.
50. Alors que l'article 12, paragraphe 2, dispose que les mesures visant à faire respecter les restrictions contenues dans les conditions générales sont proportionnées, des garanties supplémentaires sont nécessaires pour veiller à ce que les mesures de détection et de repérage des infractions potentielles restent limitées à ce qui est nécessaire.
51. Premièrement, le CEPD recommande d'étendre l'exigence prévue à l'article 12, paragraphe 2, **à toutes les formes de modération du contenu**, que cette modération ait

lieu conformément aux conditions générales du fournisseur ou à toute autre base. En outre, il convient de préciser que les mesures doivent être «nécessaires» en plus d’être «proportionnées» aux objectifs poursuivis<sup>43</sup>.

52. L’exigence selon laquelle le traitement doit être à la fois nécessaire et proportionné implique également que les mesures en question soient aussi ciblées que possible et conçues conformément à des principes tels que la **minimisation des données** et empêchent, **par défaut**, la collecte et la divulgation de données à caractère personnel, conformément à l’article 25 du règlement (UE) 2016/679<sup>44</sup>. Le CEPD rappelle que toutes les formes de modération de contenu ne nécessitent pas l’attribution à une personne concernée spécifique. Dans la mesure du possible, aucune donnée à caractère personnel ne devrait être traitée lors de la modération de contenu<sup>45</sup>.
53. Le CEPD rappelle que la proposition ne vise pas à imposer ou à exercer une surveillance générale légitime des activités en ligne des particuliers. **Toutefois, la surveillance des personnes sur l’internet étant déjà caractéristique, surtout sur les plateformes en ligne, il existe un risque d’aggravation de la situation si les mesures adoptées ne sont pas proportionnées**<sup>46</sup>. **Dans un domaine aussi délicat, le droit de l’Union doit être aussi précis et clair que possible.**
54. Le CEPD a déjà souligné précédemment que les outils automatisés de détection des éventuels contenus illicites ne devraient être utilisés que de manière **prudente et ciblée**, sur la base des conclusions de l’évaluation des risques, sous réserve d’un examen et d’un rapport périodiques<sup>47</sup>. Le CEPD note également que, conformément aux lignes directrices du comité européen de la protection des données concernant l’analyse d’impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est «susceptible d’engendrer un risque élevé», les systèmes automatisés de modération de contenu sont susceptibles de remplir plusieurs critères qui indiqueraient que la réalisation d’une AIPD est requise<sup>48</sup>. Le CEPD recommande d’exiger de toutes les plateformes en ligne utilisant des outils automatisés de modération de contenu qu’elles publient l’AIPD qui en résulte (ou, au minimum, les risques recensés et les mesures d’atténuation qui y sont associées).
55. **Le CEPD recommande de préciser que la modération de contenu ne doit pas impliquer la surveillance ou le profilage du comportement des personnes, à moins que le fournisseur ne puisse démontrer, sur la base d’une évaluation des risques, que ces mesures sont strictement nécessaires pour atténuer les catégories de risques systémiques définies à l’article 26 de la proposition (à savoir la diffusion de «contenus illicites»<sup>49</sup>; les effets négatifs sur l’exercice des droits fondamentaux; la manipulation intentionnelle du service).** Cela permettrait de préciser que l’utilisation de ces techniques a) doit faire l’objet d’un examen plus strict et b) délimite les types de préjudices susceptibles de justifier l’utilisation de ces techniques dans le contexte de la modération de contenu. Il va sans dire que toute utilisation du profilage ou de la prise de décision automatisée devrait rester soumise aux exigences du règlement (UE) 2016/679 et au contrôle des autorités de surveillance compétentes<sup>50</sup>.
56. Enfin, le CEPD recommande de préciser que tout fournisseur de services d’hébergement utilisant des moyens automatisés de modération de contenu devrait veiller à ce que ces derniers **ne produisent pas de résultats discriminatoires ou injustifiés**<sup>51</sup>.



### 3.7 Notification de soupçons d'infractions pénales

57. L'article 21 exige des plateformes en ligne qu'elles informent promptement les services répressifs et judiciaires d'informations permettant de soupçonner qu'une infraction pénale grave impliquant une menace pour la vie ou la sécurité des personnes a été commise, est commise ou est susceptible de l'être. Le considérant (48) mentionne, à titre d'exemple, les infractions définies dans la directive relative à la lutte contre les abus sexuels commis sur des enfants (directive 2011/93/UE). Dans de tels cas, la plateforme en ligne devrait informer sans délai les autorités répressives compétentes de ces soupçons, en fournissant toutes les informations pertinentes dont elle dispose.
58. Le CEPD se félicite de la définition claire des infractions pénales susceptibles de donner lieu à une obligation de signalement, à savoir les *«infractions pénales graves impliquant une menace pour la vie ou la sécurité des personnes»*. Afin de satisfaire aux exigences de sécurité juridique, y compris de prévisibilité, le CEPD **recommande vivement de préciser davantage**, en les énumérant dans une annexe, **toutes les autres infractions pénales** (qui ne sont pas des abus sexuels commis sur des enfants) qui atteignent ce seuil et peuvent donner lieu à une obligation de notification.
59. Le CEPD se félicite de la clarification explicite, au considérant (48), selon laquelle la **proposition ne fournit pas de base juridique pour le profilage des bénéficiaires des services en vue de l'identification éventuelle d'infractions pénales par les plateformes en ligne**, ainsi que de la confirmation selon laquelle il convient que les plateformes en ligne respectent également les autres règles applicables du droit de l'Union ou du droit national relatives à la protection des droits et libertés des personnes lorsqu'elles informent les services répressifs.
60. Le CEPD fait observer que la proposition ne contient aucune disposition visant à limiter l'obligation de transparence ou l'exercice des droits des personnes concernées en vertu du règlement (UE) 2016/679. Dans la mesure où la proposition est «sans préjudice» du règlement (UE) 2016/679, les obligations du fournisseur d'informer les personnes et de tenir compte des droits des personnes concernées restent donc en principe inchangées. Néanmoins, le CEPD recommande au législateur d'**introduire des mesures supplémentaires pour garantir la transparence et l'exercice des droits des personnes concernées**, sous réserve, lorsque cela est strictement nécessaire, de restrictions précisément définies (par exemple, si nécessaire, pour protéger la confidentialité d'une enquête en cours). Ces restrictions doivent, en tout état de cause, être conformes aux exigences énoncées à l'article 23, paragraphes 1 et 2, du règlement (UE) 2016/679<sup>52</sup>.
61. La proposition ne fournit pas de définition des «informations pertinentes» dont dispose la plateforme en ligne dans le cadre de la notification. Le considérant (48) mentionne, à titre d'exemple, «le contenu en question et les motifs donnant naissance à ses soupçons». Le CEPD estime qu'une **définition claire des «informations pertinentes» est nécessaire** pour garantir la sécurité juridique de toutes les parties concernées, y compris les plateformes elles-mêmes. Le CEPD recommande donc de **définir clairement le terme «informations pertinentes»**, en fournissant une liste exhaustive des catégories de données qui devraient être communiquées, ainsi que de toutes les catégories de données qui devraient être conservées en vue de faciliter la poursuite des enquêtes menées par les services répressifs compétents, le cas échéant<sup>53</sup>.

### 3.8 Transparence de la publicité en ligne

62. L'article 24 impose aux plateformes en ligne de veiller à ce que les bénéficiaires du service puissent identifier, pour chaque publicité spécifique, la personne physique ou morale *pour le compte de laquelle* la publicité est affichée, et obtenir des informations utiles concernant les *principaux paramètres* utilisés pour déterminer le bénéficiaire auquel la publicité est présentée. L'article 30 précise que les très grandes plateformes en ligne mettent en outre à la disposition du public, par l'intermédiaire d'interfaces de programme d'application, un registre contenant les mêmes informations, ainsi que des informations supplémentaires afin d'accroître davantage encore la transparence.
63. Le CEPD soutient fermement l'objectif des articles 24 et 30, qui visent à accroître la transparence et, partant, la responsabilité en ce qui concerne la publicité ciblée d'une manière qui est **complémentaire à la législation en matière de protection des données** (par exemple, en prévoyant que les informations pertinentes doivent être fournies au bénéficiaire en temps réel et en exigeant un registre public des très grandes plateformes en ligne)<sup>54</sup>. Le CEPD se félicite également que le considérant (52) précise que les articles 24 et 30 sont sans préjudice de l'application des dispositions pertinentes du règlement (UE) 2016/679 et de la directive 2002/58/CE. Enfin, le CEPD se félicite également de la référence à la nécessité d'obtenir le consentement de la personne concernée avant le traitement de données à caractère personnel à des fins de publicité ciblée.
64. Tant les articles 24 que 30 exigent des plateformes en ligne qu'elles fournissent des informations sur la «**personne physique ou morale pour le compte de laquelle la publicité est affichée**». Toutefois, il est difficile de déterminer avec certitude si c'est l'annonceur (par exemple, la société dont les produits ou services font l'objet d'une publicité) ou d'éventuels tiers qui pourraient avoir diffusé la publicité sur la plateforme en ligne (par exemple, une plateforme publicitaire<sup>55</sup>). Le CEPD recommande donc de clarifier davantage cette exigence.
65. Le CEPD note que la plupart, mais pas la totalité, de la publicité en ligne est gérée automatiquement. Le CEPD recommande d'ajouter aux exigences de l'article 24 un nouvel élément indiquant aux personnes concernées **si la publicité a été sélectionnée au moyen d'un système automatisé** (par exemple, échange ou plateforme publicitaire) et, dans ce cas, les informant de l'identité **de la ou des personnes physiques ou morales responsables** du ou des systèmes (qui peuvent être une ou plusieurs autres parties différentes de la personne physique ou morale «pour le compte de laquelle» la publicité est affichée).
66. L'article 30, paragraphe 2, point d), exige des très grandes plateformes en ligne qu'elles incluent dans le registre des informations sur «le fait que la publicité était ou non destinée à être présentée spécifiquement pour un ou plusieurs groupes particuliers de bénéficiaires du service et, dans l'affirmative, les principaux paramètres utilisés à cette fin». Le CEPD est d'avis que **les critères d'exclusion sont au moins aussi pertinents que les critères d'inclusion**, en particulier en vue de détecter une éventuelle iniquité ou un éventuel effet discriminatoire. Le CEPD recommande donc de préciser que le registre devrait également contenir des informations indiquant si un ou plusieurs groupes particuliers de bénéficiaires du service ont été *exclus* du groupe cible de la publicité.

67. Afin de garantir une véritable transparence, le CEPD suggère de remplacer les «principaux paramètres» par les «paramètres» et d'apporter des précisions supplémentaire sur **les paramètres qui devraient être divulgués au minimum pour constituer des «informations utiles»** au sens des articles 24 et 30. En particulier, le CEPD recommande d'exiger de la transparence pour chacun des critères utilisés pour cibler la publicité.
68. Afin de garantir la **responsabilité des annonceurs**, le CEPD recommande d'envisager des exigences similaires à celles qui s'appliquent pour garantir la traçabilité des professionnels (article 22) en ce qui concerne les utilisateurs de services de publicité en ligne (articles 24 et 30)<sup>56</sup>.
69. Compte tenu des nombreux risques associés à la publicité ciblée en ligne<sup>57</sup>, le CEPD exhorte le législateur à envisager d'adopter des **règles supplémentaires allant au-delà de la transparence**. À cet égard, le CEPD soutient fermement la résolution du Parlement européen, dans laquelle ce dernier considère que la publicité ciblée doit être **réglementée de manière plus stricte** au profit de formes publicitaires moins intrusives ne nécessitant pas un suivi des interactions des utilisateurs avec du contenu<sup>58</sup>. Par conséquent, le CEPD demande aussi instamment au législateur d'envisager une **suppression progressive débouchant sur une interdiction de la publicité ciblée reposant sur un suivi omniprésent**<sup>59</sup>.
70. Enfin, pour compléter ce qui précède, le CEPD invite le législateur à envisager des restrictions supplémentaires concernant a) les **catégories de données qui peuvent être traitées à des fins de ciblage** (par exemple des restrictions concernant les données collectées «hors plateforme»); b) **les catégories de données ou les critères sur la base desquels des publicités peuvent être ciblées ou notifiées** (par exemple des critères qui correspondent directement ou indirectement à des catégories spéciales de données ou qui sont susceptibles d'être utilisés pour exploiter des vulnérabilités); et c) **les catégories de données susceptibles d'être divulguées** à des annonceurs ou à des tiers pour permettre ou faciliter la publicité ciblée.

### 3.9 Systèmes de recommandation

71. L'article 2, point o), définit un «système de recommandation» comme *«un système entièrement ou partiellement automatisé utilisé par une plateforme en ligne pour **suggérer** dans son interface en ligne des informations spécifiques aux bénéficiaires du service, notamment à la suite d'une recherche lancée par le bénéficiaire ou en déterminant de toute autre manière l'ordre relatif d'importance des informations affichées»*. Le CEPD estime que, dans la pratique, les systèmes de recommandation **font bien plus que «suggérer»** des contenus en ligne. En effet, le considérant (62) explique que les systèmes de recommandation peuvent *«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 bénéficiaires»*.
72. Le CEPD se félicite de la reconnaissance du fait que les systèmes de recommandation **peuvent avoir une incidence significative** sur la capacité des bénéficiaires à récupérer les informations en ligne et à interagir avec elles et jouent également un rôle important dans **l'amplification** de certains messages, la diffusion virale de l'information et la stimulation du comportement en ligne<sup>60</sup>. Certains systèmes de recommandation se nourrissent des

profils des personnes concernées et définissent le contenu auquel elles peuvent accéder sur les plateformes en ligne, avec tous les risques que cela comporte.

73. Les risques de profilage et de microciblage dans le contexte des systèmes de recommandation ou de publicité en ligne ont déjà été soulevés par le CEPD dans son avis sur la manipulation en ligne et les données à caractère personnel<sup>61</sup>. Le CEPD recommande au législateur de l'Union de préciser que, conformément aux exigences en matière de protection des données dès la conception et par défaut, les systèmes de recommandation **ne devraient pas, par défaut, être fondés sur le «profilage»** au sens de l'article 4, paragraphe 4, du règlement (UE) 2016/679.
74. L'article 29, paragraphe 1, prévoit que les très grandes plateformes en ligne qui utilisent des systèmes de recommandation veillent à ce que les bénéficiaires du service aient au minimum la possibilité de recourir à un système de recommandation qui ne relève pas du profilage, au sens de l'article 4, paragraphe 4, du règlement (UE) 2016/679. Conformément aux exigences en matière de protection des données dès la conception et par défaut et de minimisation des données, le CEPD recommande vivement de remplacer le **principe du retrait du consentement (opt-out) par celui du consentement préalable (opt-in)**, en faisant de l'option non basée sur le profilage l'option par défaut.
75. L'article 29, paragraphe 1, impose aux très grandes plateformes en ligne d'établir, dans leurs conditions générales, les «principaux paramètres» utilisés dans leurs systèmes de recommandation, ainsi que les options dont disposent les bénéficiaires du service pour modifier ou influencer ces principaux paramètres qu'elles auraient rendus accessibles. Nonobstant l'exigence selon laquelle les informations doivent être présentées «de manière claire, accessible et aisément compréhensible», le CEPD considère que les **conditions générales sont généralement des documents longs et légalistes** que les utilisateurs moyens ont du mal à comprendre. Les conditions générales des très grandes plateformes en ligne sont souvent encore plus complexes parce qu'elles fournissent des informations sur les nombreux services connexes que propose la plateforme. Par conséquent, si des informations sur les paramètres et les options du système de recommandation étaient incluses dans les conditions générales, les personnes concernées auraient encore plus de mal à les trouver et à les comprendre. Le CEPD recommande vivement d'exiger que ces informations concernant le rôle et le fonctionnement des systèmes de recommandation soient présentées séparément, d'une manière aisément accessible, claire pour les utilisateurs moyens et concise.
76. Dans le même ordre d'idées que les recommandations relatives à la transparence de la publicité en ligne, il est également nécessaire de garantir une **véritable transparence dans le contexte des systèmes de recommandation et de leur utilisation des profils des personnes concernées**. Par conséquent, le CEPD recommande de remplacer les «principaux paramètres» par les «paramètres» ou, à tout le moins, d'apporter des précisions supplémentaires sur les paramètres qui devraient être divulgués au minimum pour constituer des «informations utiles» dans ce contexte<sup>62</sup>.
77. Malgré leur impact significatif, les systèmes de recommandation sont sans friction du point de vue de l'utilisateur. Afin d'améliorer la transparence et le contrôle des utilisateurs, le CEPD recommande d'inclure les exigences supplémentaires suivantes à l'article 29:

- indiquer dans une partie bien visible de la plateforme que celle-ci utilise un système de recommandation et proposer des contrôles avec les options disponibles de manière conviviale;
- indiquer à l'utilisateur de la plateforme si le système de recommandation est un système automatisé et, dans ce cas, l'informer de l'identité de la personne physique ou morale responsable du système, si elle est différente du fournisseur de la plateforme;
- permettre aux personnes concernées de visualiser, de manière conviviale, tout profil ou profils utilisés aux fins de la curation du contenu de la plateforme pour le bénéficiaire du service;
- permettre aux bénéficiaires du service de personnaliser les systèmes de recommandation au moins compte tenu de critères naturels de base (par exemple, le temps, les sujets d'intérêt, etc.); et
- offrir aux utilisateurs une option facilement accessible pour supprimer tout profil ou profils utilisés pour la curation du contenu qu'ils voient.

### 3.10 Accès des chercheurs agréés

78. L'article 31 dispose que, sur demande motivée du coordinateur de l'État membre d'établissement pour les services numériques ou de la Commission, les très grandes plateformes en ligne fournissent, dans un délai raisonnable, comme spécifié dans la demande, l'accès aux données à des «chercheurs agréés», à seule fin de procéder à des recherches contribuant à l'identification et à la compréhension des risques systémiques au sens de l'article 26, paragraphe 1.
79. Le CEPD se félicite de l'objectif de la proposition de soumettre les très grandes plateformes en ligne au contrôle des «chercheurs agréés», conformément au règlement (UE) 2016/679<sup>63</sup>. Le CEPD recommande à la Commission d'appliquer des normes strictes lorsqu'elle détermine les critères permettant de considérer un chercheur comme étant «*indépendant de tous intérêts commerciaux*».
80. La recherche scientifique remplit une fonction précieuse dans une société démocratique: elle permet de demander des comptes aux acteurs puissants. Le CEPD rappelle que la **protection des données ne doit pas être détournée pour permettre aux acteurs puissants d'échapper à la transparence et à la responsabilité**. Les chercheurs opérant dans des cadres de gouvernance éthique devraient donc être en mesure d'accéder aux API nécessaires et à d'autres données, avec une base juridique valable et sous réserve du principe de proportionnalité et des garanties appropriées<sup>64</sup>.
81. Le CEPD note qu'en vertu de la proposition, les chercheurs agréés seraient autorisés à enquêter sur les risques systémiques présentés à l'article 26 (article 31, paragraphe 2). Le CEPD se félicite que la proposition incluse à l'article 26 à la fois les risques systémiques pour les droits individuels et les préoccupations sociétales, mais il invite instamment le législateur à préciser davantage quels sont les «risques systémiques» et les «préjudices pour la société» (considérants 54, 56 et 94). En ce qui concerne l'article 26, paragraphe 1, point c), le CEPD note que les services des très grandes plateformes en ligne peuvent présenter des risques systémiques pour «la protection de la santé publique, des mineurs, du discours civique ou des effets avérés ou prévisibles en lien avec les processus électoraux et la sécurité publique», qu'ils soient manipulés ou non. Le CEPD suggère donc de reformuler

ce paragraphe comme suit: «(c) des effets négatifs systémiques, avérés ou prévisibles, sur la protection de la santé publique, des mineurs, du discours civique ou des effets avérés ou prévisibles en lien avec les processus électoraux et la sécurité publique, **notamment en ce qui concerne le risque de manipulation intentionnelle de leur service, y compris via l'utilisation non authentique ou l'exploitation automatisée du service**».

82. Le CEPD estime que le champ d'application de l'article 31 est restreint, étant donné que l'accès est donné à des chercheurs agréés, à seule fin de procéder à des recherches contribuant à *l'identification et à la compréhension* des risques systémiques tels que définis à l'article 26, paragraphe 1, dans le cadre de l'évaluation et du contrôle du respect de la proposition. Le CEPD estime que l'article 31 devrait être élargi pour permettre à tout le moins de **vérifier l'efficacité et la proportionnalité des mesures d'atténuation**.
83. Enfin, le CEPD recommande au colégislateur d'envisager des moyens de **faciliter plus généralement la recherche d'intérêt public**, y compris en dehors du cadre du contrôle du respect de la proposition (et, en outre, la fourniture d'API accessibles au public pour la publicité en ligne), à condition que cette recherche soit véritablement menée dans l'intérêt public. Dans ce contexte, le CEPD renvoie également à son avis préliminaire sur la protection des données et la recherche scientifique<sup>65</sup>.

### 3.11 Interopérabilité des plateformes

84. Le CEPD estime que les problèmes d'amplification algorithmique et d'autres préjudices que la proposition vise à examiner sont exacerbés par le caractère fermé des très grandes plateformes en ligne, qui limite la capacité des utilisateurs à communiquer entre les plateformes («walled gardens» ou écosystèmes fermés). Une interopérabilité accrue peut faciliter le développement d'un environnement plus ouvert et pluraliste et créer de nouvelles possibilités de développement de services numériques innovants.
85. Le CEPD recommande au colégislateur d'envisager d'introduire des exigences minimales d'interopérabilité pour les très grandes plateformes en ligne, avec l'obligation explicite pour ces dernières 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 très grandes plateformes en ligne (dans ses différentes spécifications, à savoir l'interopérabilité des protocoles, l'interopérabilité des données, l'interopérabilité complète des protocoles<sup>66</sup>). 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<sup>67</sup>.

### 3.12 Mise en œuvre, coopération, sanctions et exécution

86. Le CEPD se félicite de la reconnaissance de la **pertinence intersectorielle** des aspects régis par la proposition, y compris en ce qui concerne la protection des personnes physiques à l'égard du traitement des données à caractère personnel. Certaines dispositions et mesures éventuelles adoptées en vertu de la proposition auront clairement une incidence sur le

traitement des données à caractère personnel. La pertinence intersectorielle de la proposition est également démontrée par un certain nombre de dispositions, dont les articles 26 et 27 (identification et atténuation des risques systémiques), l'article 35, paragraphe 1 (codes de conduite) et l'article 36 (codes de conduite pour la publicité en ligne).

87. Le CEPD considère qu'il est nécessaire de veiller à **la complémentarité dans le contrôle** et la surveillance des plateformes en ligne et d'autres fournisseurs de services d'hébergement. Cette complémentarité est nécessaire non seulement pour atténuer les risques d'atteinte non justifiée aux droits fondamentaux, mais aussi pour accroître la transparence et la responsabilité des acteurs, qui sont régies par la proposition. Fort de l'expérience acquise en ce qui concerne la Digital Clearinghouse<sup>68</sup>, le CEPD recommande vivement, dans la proposition, de:
- (1) prévoir une **base juridique explicite pour la coopération** entre les autorités compétentes, chacune agissant dans leurs domaines de compétence respectifs;
  - (2) exiger une coopération **institutionnalisée et structurée** entre les autorités de contrôle compétentes, y compris les autorités chargées de la protection des données;
  - (3) **faire explicitement référence** aux **autorités** compétentes qui coopèrent et définir les **circonstances dans lesquelles la coopération devrait avoir lieu**.
88. Déjà au considérant (91), il est indiqué que le comité européen des services numériques 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 la protection des données et la protection des consommateurs, dans la mesure où cela est nécessaire à l'accomplissement de ses tâches. Compte tenu de l'importance de la coopération avec les **autorités compétentes dans le domaine du droit de la concurrence**, le CEPD recommande d'ajouter ici une référence explicite à ces autorités, en plus de celles déjà mentionnées. Le CEPD recommande également d'introduire dans les considérants de la proposition une **référence explicite au comité européen de la protection des données**.
89. Le CEPD recommande de veiller à ce que les coordinateurs pour les services numériques, les autres autorités compétentes et la Commission aient également le pouvoir et le devoir de consulter les autorités compétentes concernées, y compris les autorités chargées de la protection des données, **dans le cadre de leurs enquêtes et évaluations** du respect de la proposition. En outre, le CEPD recommande de préciser que les autorités de contrôle compétentes en vertu de la proposition devraient être en mesure de fournir aux autorités de contrôle compétentes en vertu du règlement (UE) 2016/679, sur demande ou de leur propre initiative, toute **information obtenue dans le cadre d'audits et d'enquêtes** ayant trait au traitement de données à caractère personnel et d'inclure une **base juridique explicite** à cet effet.
90. Parmi les autres circonstances dans lesquelles la coopération devrait avoir lieu figurent, sans s'y limiter:
- l'identification et l'évaluation des risques systémiques les plus importants et récurrents, ainsi que les bonnes pratiques en vue de l'atténuation de ces risques (article 27, paragraphes 2 et 3);

- des codes de conduite pour tenir compte des difficultés liées à différents types de contenus illicites et de risques systémiques (article 35); ainsi que
- des codes de conduite pour la publicité en ligne (article 36).

91. L'article 41, paragraphe 5, dispose que «[l]es 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*». L'article 42, paragraphe 2, dispose que les sanctions sont «effectives, proportionnées et dissuasives». Par souci de cohérence, le CEPD recommande également de se référer aux critères pertinents énoncés à l'article 59 (amendes infligées par la Commission).

92. L'article 49, paragraphe 1, point d), dispose que le Comité «conseille la Commission en ce qui concerne les mesures à prendre au titre de l'article 51 et, *lorsque la Commission le demande*, adopte des avis sur les projets de *mesures* de la Commission concernant les très grandes plateformes en ligne conformément au présent règlement». Le CEPD recommande de permettre au Comité 1) d'émettre des avis d'initiative et 2) d'émettre des avis sur des questions autres que les *mesures* prises par la Commission.

## 4. CONCLUSIONS

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

***En ce qui concerne le lien avec le règlement (UE) 2016/679 et la directive 2002/58/CE:***

- aligner le libellé de l'article 1<sup>er</sup>, paragraphe 5, point i), de la proposition sur celui de l'article 1<sup>er</sup>, paragraphe 5, point b), de la directive 2000/31/CE; et
- préciser que la proposition ne s'applique pas aux questions relatives à la responsabilité des responsables du traitement et des sous-traitants;

***En ce qui concerne la modération des contenus et la notification des soupçons d'infractions pénales:***

- préciser que toutes les formes de modération des contenus ne nécessitent pas l'attribution à une personne concernée spécifique et que, conformément aux exigences de minimisation des données et de protection des données dès la conception et par défaut, la modération de contenu ne devrait, dans la mesure du possible, impliquer aucun traitement de données à caractère personnel;
- veiller à ce que la modération des contenus se fasse dans le respect de l'État de droit, en déterminant dans quels cas les efforts de lutte contre les «contenus illicites» légitiment l'utilisation de moyens automatisés et le traitement de données à caractère personnel pour détecter, recenser et combattre les contenus illicites;



- préciser que le profilage à des fins de modération de contenu devrait être interdit, à moins que le fournisseur ne puisse démontrer que de telles mesures sont strictement nécessaires pour faire face aux risques systémiques explicitement déterminés par la proposition;
- préciser si, et le cas échéant, dans quelle mesure, les fournisseurs de services intermédiaires sont autorisés à notifier volontairement aux services répressifs ou judiciaires des soupçons d'infractions pénales, en dehors du cas prévu à l'article 21 de la proposition;
- préciser que tout fournisseur de services d'hébergement utilisant des moyens automatisés de modération de contenu devrait veiller à ce que ces moyens ne produisent pas de résultats discriminatoires ou injustifiés;
- étendre l'exigence prévue à l'article 12, paragraphe 2, de la proposition à toutes les formes de modération du contenu, que cette modération ait lieu conformément aux conditions générales du fournisseur ou à toute autre base; et préciser que les mesures doivent être «nécessaires» en plus d'être «proportionnées» aux objectifs poursuivis;
- renforcer les exigences de transparence énoncées à l'article 14, paragraphe 6, et à l'article 15, paragraphe 2, point c), de la proposition, en précisant davantage les informations à fournir aux personnes concernées, en particulier en cas d'utilisation de moyens automatisés pour la modération de contenu, sans préjudice de l'obligation d'information et des droits des personnes concernées en vertu du règlement (UE) 2016/679;
- modifier l'article 15, paragraphe 2, de la proposition pour indiquer sans ambiguïté que des informations relatives à l'utilisation de moyens automatisés pour détecter et repérer des contenus illicites doivent en tout état de cause être fournies, indépendamment de la question de savoir si la décision prise ultérieurement impliquait l'utilisation de moyens automatisés ou non;
- exiger de tous les fournisseurs de services d'hébergement, et pas seulement des plateformes en ligne, qu'ils mettent en place un mécanisme de réclamation facilement accessible, comme le prévoit l'article 17 de la proposition;
- insérer à l'article 17 de la proposition un délai dans lequel la plateforme doit rendre la décision relative à la réclamation, ainsi que l'indication selon laquelle le mécanisme de réclamation qui doit être mis en place est sans préjudice des droits et voies de recours dont disposent les personnes concernées conformément au règlement (UE) 2016/679 et à la directive 2002/58/CE;
- préciser davantage, en les énumérant dans une annexe, toutes les autres infractions pénales (qui ne sont pas des abus sexuels commis sur des enfants) qui atteignent le seuil fixé à l'article 21 de la proposition et qui peuvent donner lieu à une obligation de notification;
- envisager d'introduire des mesures supplémentaires pour garantir la transparence et l'exercice des droits des personnes concernées, sous réserve, lorsque cela est strictement nécessaire, de restrictions précisément définies (par exemple, si nécessaire,

pour protéger la confidentialité d'une enquête en cours), conformément aux exigences énoncées à l'article 23, paragraphes 1 et 2 du règlement (UE) 2016/679; et

- définir clairement le terme «informations pertinentes», mentionné à l'article 21 de la proposition, en fournissant une liste exhaustive des catégories de données qui devraient être communiquées, ainsi que de toutes les catégories de données qui devraient être conservées en vue de faciliter la poursuite des enquêtes menées par les services répressifs compétents, le cas échéant.

***En ce qui concerne la publicité en ligne:***

- envisager des règles supplémentaires allant au-delà de la transparence, y compris une suppression progressive débouchant sur une interdiction de la publicité ciblée reposant sur un suivi omniprésent;
- envisager des restrictions concernant a) les catégories de données qui peuvent être traitées à des fins de ciblage; b) les catégories de données ou les critères sur la base desquels des publicités peuvent être ciblées ou notifiées; et c) les catégories de données susceptibles d'être divulguées à des annonceurs ou à des tiers pour permettre ou faciliter la publicité ciblée; et
- aux articles 24 et 30 de la proposition, préciser davantage la référence à la personne physique ou morale pour le compte de laquelle la publicité est affichée;
- ajouter aux exigences de l'article 24 un nouvel élément exigeant du fournisseur de la plateforme qu'il indique aux personnes concernées si la publicité a été sélectionnée au moyen d'un système automatisé (par exemple, échange ou plateforme publicitaire) et, dans ce cas, l'identité de la ou des personnes physiques ou morales responsables du ou des systèmes;
- préciser à l'article 30, paragraphe 2, point d), que le registre devrait également contenir des informations indiquant si un ou plusieurs groupes particuliers de bénéficiaires du service ont été *exclus* du groupe cible de la publicité;
- remplacer les «principaux paramètres» par les «paramètres» et apporter des précisions supplémentaires sur les paramètres qui devraient être divulgués au minimum pour constituer des «informations utiles» au sens des articles 24 et 30 de la proposition; et
- envisager des exigences similaires à celles qui s'appliquent pour garantir la traçabilité des professionnels (article 22 de la proposition) en ce qui concerne les utilisateurs de services de publicité en ligne (articles 24 et 30 de la proposition).

***En ce qui concerne les systèmes de recommandation:***

- préciser que, conformément aux exigences en matière de protection des données dès la conception et par défaut, les systèmes de recommandation ne devraient pas être fondés sur le «profilage» au sens de l'article 4, paragraphe 4, du règlement (UE) 2016/679;

- veiller à ce que les informations relatives au rôle et au fonctionnement des systèmes de recommandation soient présentées séparément, de manière à être facilement accessibles, claires pour le profane et concises;
- veiller à ce que, conformément aux exigences en matière de protection des données dès la conception et par défaut, les systèmes de recommandation ne soient pas fondés sur le «profilage» au sens de l'article 4, paragraphe 4, du règlement (UE) 2016/679; et
- introduire les exigences supplémentaires suivantes à l'article 29 de la proposition:
  - indiquer dans une partie bien visible de la plateforme que celle-ci utilise un système de recommandation et proposer un contrôle avec les options disponibles d'une manière conviviale;
  - indiquer à l'utilisateur de la plateforme si le système de recommandation est un système de prise de décision automatisé et, dans ce cas, l'informer de l'identité de la personne physique ou morale responsable de la décision.
  - permettre aux personnes concernées de visualiser, de manière conviviale, tout profil ou profils utilisés aux fins de la curation du contenu de la plateforme pour le bénéficiaire du service;
  - permettre aux bénéficiaires du service de personnaliser les systèmes de recommandation au moins compte tenu de critères naturels de base (par exemple, le temps, les sujets d'intérêt, etc.); et
  - offrir aux utilisateurs une option facilement accessible pour supprimer tout profil ou profils utilisés pour la curation du contenu qu'ils voient.

***En ce qui concerne l'accès des chercheurs agréés:***

- veiller à ce que, conformément aux exigences en matière de protection des données dès la conception et par défaut, les systèmes de recommandation ne soient pas fondés sur le «profilage» au sens de l'article 4, paragraphe 4, du règlement (UE) 2016/679;
- reformuler l'article 26, paragraphe 1, point c), de la proposition afin de faire référence aux effets négatifs systémiques, avérés ou prévisibles, sur la protection de la santé publique, des mineurs, du discours civique ou des effets avérés ou prévisibles en lien avec les processus électoraux et la sécurité publique, notamment en ce qui concerne le risque de manipulation intentionnelle de leur service, y compris via l'utilisation non authentique ou l'exploitation automatisée du service;
- étendre l'article 31 afin de permettre à tout le moins de vérifier l'efficacité et la proportionnalité des mesures d'atténuation; et
- envisager des moyens de faciliter plus généralement la recherche d'intérêt public, y compris en dehors du cadre du contrôle du respect de la proposition;

***En ce qui concerne l'interopérabilité des plateformes:***

- envisager d'introduire des exigences minimales d'interopérabilité pour les très grandes plateformes en ligne et promouvoir l'élaboration de normes techniques au niveau

européen, conformément à la législation de l'Union applicable en matière de normalisation européenne.

***En ce qui concerne la mise en œuvre, la coopération, les sanctions et l'exécution:***

- garantir la complémentarité dans le contrôle et la surveillance des plateformes en ligne et d'autres fournisseurs de services d'hébergement, notamment:
  - en prévoyant une base juridique explicite pour la coopération entre les autorités compétentes, chacune agissant dans leurs domaines de compétence respectifs;
  - en exigeant une coopération institutionnalisée et structurée entre les autorités de contrôle compétentes, y compris les autorités chargées de la protection des données; et
  - en faisant explicitement référence aux autorités compétentes qui ont coopérer et en définissant les circonstances dans lesquelles la coopération devrait avoir lieu.
- faire référence, dans les considérants de la proposition, aux autorités compétentes dans le domaine du droit de la concurrence, ainsi qu'au comité européen de la protection des données;
- veiller à ce que les coordinateurs pour les services numériques, les autorités compétentes et la Commission aient également le pouvoir et le devoir de consulter les autorités compétentes concernées, y compris les autorités chargées de la protection des données, dans le cadre de leurs enquêtes et évaluations du respect de la proposition;
- préciser que les autorités de contrôle compétentes en vertu de la proposition devraient être en mesure de fournir, à la demande des autorités de contrôle compétentes en vertu du règlement (UE) 2016/679 ou de leur propre initiative, toute information obtenue dans le cadre des audits et enquêtes ayant trait au traitement de données à caractère personnel et inclure une base juridique explicite à cet effet;
- garantir une plus grande cohérence entre les critères énoncés à l'article 41, paragraphe 5, à l'article 42, paragraphe 2, et à l'article 59 de la proposition; et
- permettre au comité européen pour les services numériques d'émettre des avis d'initiative et des avis sur des questions autres que les mesures prises par la Commission.

Bruxelles, le 10 février 2021

Wojciech Wiewiorowski

*(signature électronique)*

## Notes

---

<sup>1</sup> JO L 119 du 4.5.2016, p. 1.

<sup>2</sup> JO L 295 du 21.11.2018, p. 39.

<sup>3</sup> COM(2020) 825 final.

<sup>4</sup> COM(2020) 67 final, p. 12.

<sup>5</sup> COM (2020) 825 final, p. 1.

<sup>6</sup> COM (2020) 825 final, p. 2.

<sup>7</sup> COM(2020) 842 final.

<sup>8</sup> Contrôleur européen de la protection des données, «The EDPS Strategy 2020-2024, Shaping a Safer Digital Future», [Stratégie du CEPD pour 2020-2024, Façonner un avenir numérique plus sûr], 30 juin 2020, [https://edps.europa.eu/press-publications/press-news/press-releases/2020/shaping-safer-digital-future-new-strategy-new\\_fr](https://edps.europa.eu/press-publications/press-news/press-releases/2020/shaping-safer-digital-future-new-strategy-new_fr)

<sup>9</sup> COM (2020) 825 final, p. 12 («*Les citoyens de l'Union et les autres citoyens sont exposés en ligne à des risques et à des préjudices toujours plus importants, qu'il s'agisse de la diffusion de contenus et d'activités illégaux, de la limitation de la liberté d'expression ou d'autres préjudices pour la société*»).

<sup>10</sup> Considérant (54) de la proposition.

<sup>11</sup> Contrôleur européen de la protection des données, avis n° 3/2018 sur la manipulation en ligne et les données à caractère personnel, 19 mars 2018, [https://edps.europa.eu/sites/edp/files/publication/18-03-19\\_online\\_manipulation\\_fr.pdf](https://edps.europa.eu/sites/edp/files/publication/18-03-19_online_manipulation_fr.pdf).

<sup>12</sup> Comité européen de la protection des données, Lignes directrices 8/2020 relatives au ciblage des utilisateurs de médias sociaux, Version 1.0, 2 septembre 2020, 4-7, [https://edpb.europa.eu/sites/edpb/files/consultation/edpb\\_guidelines\\_202008\\_onthetargetingofsocialmediausers\\_en.pdf](https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202008_onthetargetingofsocialmediausers_en.pdf).

<sup>13</sup> Considérant (56) de la proposition.

<sup>14</sup> Considérant (68) de la proposition.

<sup>15</sup> Voir également, dans le même ordre d'idées, la note du coordinateur de l'UE pour la lutte contre le terrorisme intitulée «The role of algorithmic amplification in promoting violent and extremist content and its dissemination on platforms and social media» [Le rôle de l'amplification algorithmique dans la promotion des contenus violents et extrémistes et leur diffusion sur les plateformes et les médias sociaux], p. 2, Conseil de l'Union européenne, 9 décembre 2020, <https://data.consilium.europa.eu/doc/document/ST-12735-2020-INIT/en/pdf> («*Ce modèle économique conduit automatiquement les utilisateurs vers les contenus détectés par des algorithmes comme étant les plus attrayants. En tant que telles, les entreprises de médias sociaux ne se contentent pas d'offrir une plateforme sur laquelle les citoyens exercent leur liberté d'expression. Elles amplifient certains contenus et en rétrogradent d'autres, tout en protégeant les mécanismes qui les régissent de l'examen public*»).

<sup>16</sup> COM(2020) 842 final.

<sup>17</sup> COM (2020) 825 final, p. 5.

<sup>18</sup> Contrôleur européen de la protection des données, «Observations formelles du CEPD relatives à une proposition de directive du Parlement européen et du Conseil sur le droit d'auteur dans le marché unique numérique», 12 février 2019, p. 6, [https://edps.europa.eu/sites/edp/files/publication/18-07-03\\_edps\\_formal\\_comments\\_copyright\\_fr.pdf](https://edps.europa.eu/sites/edp/files/publication/18-07-03_edps_formal_comments_copyright_fr.pdf).

<sup>19</sup> Ibid., p. 2.

<sup>20</sup> JO L 178 du 17.7.2000, p. 1.

<sup>21</sup> Voir arrêt rendu par la Cour de justice de l'Union européenne dans l'affaire *La Quadrature du Net a.o.*, affaires jointes C-511/18, C-512/18 et C-520/18, 6 octobre 2020, ECLI:EU:C:2020:79, aux points 199 et 200 [«199 Toutefois, l'article 1<sup>er</sup>, paragraphe 5, de la directive 2000/31 dispose que celle-ci **n'est pas applicable aux questions relatives aux services de la société de l'information qui sont couvertes par les directives 95/46 et 97/66. À cet égard, il ressort des considérants 14 et 15 de la directive 2000/31 que la protection de la confidentialité des communications ainsi que des personnes physiques à l'égard du traitement des données à caractère personnel dans le cadre des services de la société de l'information est uniquement régie par les directives 95/46 et 97/66, cette dernière interdisant, à son article 5, aux fins de la protection de la confidentialité des communications, toute forme d'interception ou de surveillance des communications. 200 Ainsi, des questions liées à la protection de la confidentialité des communications et des données à caractère personnel doivent être appréciées à l'aune de la directive 2002/58 et du règlement 2016/679, ceux-ci ayant remplacé respectivement la directive 97/66 et la directive 95/46, étant précisé que la protection **que vise à assurer la directive 2000/31 ne peut en tout état de cause pas porter atteinte aux exigences résultant de la directive 2002/58 et du règlement 2016/679** (voir, en ce sens, arrêt du 29 janvier 2008, *Promusicae*, C-275/06, EU:C:2008:54, point 57)»].**

---

<sup>22</sup> En vertu de l'article 2, point g), de la proposition, on entend par «contenu illicite» *«toute information qui, en soi ou de par sa référence à une activité, y compris la vente de produits ou la prestation de services, n'est pas conforme au droit de l'Union ou au droit d'un État membre, quel qu'en soit l'objet précis ou la nature précise».*

<sup>23</sup> Article 82 du règlement (UE) 2016/679.

<sup>24</sup> Considérant (28) de la proposition.

<sup>25</sup> Voir aussi COM (2020) 825 final, p. 3.

<sup>26</sup> Voir également la lettre adressée par le comité européen de la protection des données au Dr. Alexander Dix, 20 octobre 2020, [https://edpb.europa.eu/sites/edpb/files/files/file1/out2020-0111edpb\\_replydrdixart17.pdf](https://edpb.europa.eu/sites/edpb/files/files/file1/out2020-0111edpb_replydrdixart17.pdf).

<sup>27</sup> Voir également Contrôleur européen de la protection des données, «Opinion 7/2020 on the Proposal for temporary derogations from Directive 2002/58/EC for the purpose of combatting child sexual abuse online» [Avis n° 7/2020 sur la proposition de dérogations temporaires à la directive 2002/58/CE aux fins de la lutte contre les abus sexuels commis contre des enfants en ligne], 10 novembre 2020, [https://edps.europa.eu/sites/edp/files/publication/20-11-10\\_opinion\\_combatting\\_child\\_abuse\\_en.pdf](https://edps.europa.eu/sites/edp/files/publication/20-11-10_opinion_combatting_child_abuse_en.pdf).

<sup>28</sup> Certaines obligations de base sont applicables à tous les fournisseurs de services intermédiaires. En outre, la proposition prévoit des obligations supplémentaires pour les fournisseurs de services d'hébergement et, plus particulièrement, les plateformes en ligne et les très grandes plateformes en ligne.

<sup>29</sup> Article 2, point p), de la proposition.

<sup>30</sup> Voir groupe de travail «Article 29» sur la protection des données, «Lignes directrices sur la transparence au sens du règlement 2016/679», wp260rev.01, 11 avril 2018 (adoptées ultérieurement par le comité européen de la protection des données), [https://ec.europa.eu/newsroom/article29/item-detail.cfm?item\\_id=622227](https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227).

<sup>31</sup> Voir également article 21 de la proposition.

<sup>32</sup> Voir paragraphe 49 et suivants.

<sup>33</sup> Voir article 2, point h), de la proposition.

<sup>34</sup> Article 14, paragraphe 1, de la proposition.

<sup>35</sup> Voir article 14, paragraphe 2, de la proposition.

<sup>36</sup> Voir article 14, paragraphe 4, de la proposition.

<sup>37</sup> Voir groupe de travail «Article 29» sur la protection des données, Lignes directrices relatives à la prise de décision individuelle automatisée et au profilage aux fins du règlement 2016/679, WP251rev.01, 6 février 2018 (adoptées ultérieurement par le comité européen de la protection des données), [https://ec.europa.eu/newsroom/article29/item-detail.cfm?item\\_id=612053](https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053)

<sup>38</sup> Article 15, paragraphe 2, point c), de la proposition.

<sup>39</sup> Tel qu'il est actuellement rédigé, le texte pourrait être interprété (à tort) comme suggérant que les informations relatives à l'utilisation de moyens automatisés pour détecter ou repérer des contenus illicites ne devraient être fournies que si des moyens automatisés ont également été utilisés pour prendre la décision.

<sup>40</sup> Article 15, paragraphe 4, de la proposition.

<sup>41</sup> Voir paragraphes 40 à 43 ci-dessus. C'est également ce qui est confirmé dans l'exposé des motifs de la proposition, qui prévoit que *«les dispositions du présent règlement relatives à la responsabilité ne doivent pas faire obstacle au développement ni à la mise en œuvre effective, par les différentes parties concernées, de systèmes techniques de protection et d'identification ainsi que de systèmes automatisés de reconnaissance rendus possibles par les techniques numériques, dans le respect des limites établies par le règlement (UE) 2016/679».*

<sup>42</sup> CEPD, «Observations formelles du CEPD sur la proposition de règlement du Parlement européen et du Conseil relatif à la prévention de la diffusion de contenus à caractère terroriste en ligne», 12 février 2019, p. 9, [https://edps.europa.eu/sites/edp/files/publication/2018-02-13\\_edps\\_formal\\_comments\\_online\\_terrorism\\_regulation\\_fr.pdf](https://edps.europa.eu/sites/edp/files/publication/2018-02-13_edps_formal_comments_online_terrorism_regulation_fr.pdf)

<sup>43</sup> Voir aussi Contrôleur européen de la protection des données, «Guide pour l'évaluation de la nécessité des mesures

limitant le droit fondamental à la protection des données à caractère personnel», 11 avril 2017; «Lignes directrices portant sur l'évaluation du caractère proportionné des mesures limitant les droits fondamentaux à la vie privée et à la protection des données à caractère personnel», 19 décembre 2019, [https://edps.europa.eu/sites/edp/files/publication/19-12-19\\_edps\\_proportionality\\_guidelines2\\_fr.pdf](https://edps.europa.eu/sites/edp/files/publication/19-12-19_edps_proportionality_guidelines2_fr.pdf)

<sup>44</sup> Voir, dans le même esprit, «Observations formelles du CEPD relatives à une proposition de directive du Parlement européen et du Conseil sur le droit d'auteur dans le marché unique numérique», 12 février 2019, p. 5, [https://edps.europa.eu/sites/edp/files/publication/18-07-03\\_edps\\_formal\\_comments\\_copyright\\_fr.pdf](https://edps.europa.eu/sites/edp/files/publication/18-07-03_edps_formal_comments_copyright_fr.pdf).

<sup>45</sup> Voir également la lettre adressée par le comité européen de la protection des données au Dr. Alexander Dix, 20 octobre 2020, [https://edpb.europa.eu/sites/edpb/files/files/file1/out2020-0111edpb\\_replydrdixart17.pdf](https://edpb.europa.eu/sites/edpb/files/files/file1/out2020-0111edpb_replydrdixart17.pdf).

<sup>46</sup> CEPD, «Observations formelles du CEPD relatives à une proposition de directive du Parlement européen et du Conseil sur le droit d'auteur dans le marché unique numérique», p. 6.

<sup>47</sup> CEPD, «Observations formelles du CEPD sur la proposition de règlement du Parlement européen et du Conseil relatif à la prévention de la diffusion de contenus à caractère terroriste en ligne», p. 6-7.

---

<sup>48</sup> Les lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est «susceptible d'engendrer un risque élevé» aux fins du règlement (UE) 2016/679 comprennent neuf critères. Les systèmes automatisés de modération des contenus utilisés par les plateformes en ligne qui impliquent le traitement de données à caractère personnel satisfont au moins aux trois premiers critères (évaluation ou notation, prise de décisions automatisée avec effet juridique ou effet similaire significatif et surveillance systématique). Les très grandes plateformes en ligne remplissent également le critère du traitement à grande échelle.

<sup>49</sup> Comme indiqué précédemment, le CEPD recommande au colégislateur de définir davantage les circonstances dans lesquelles les efforts de lutte contre le «contenu illicite» légitiment le traitement de données à caractère personnel. Voir en particulier paragraphes 26-27.

<sup>50</sup> Voir aussi groupe de travail «Article 29» sur la protection des données, «Lignes directrices relatives à la prise de décision individuelle automatisée et au profilage aux fins du règlement (UE) 2016/679», wp251rev.01, 6 février 2018 (adoptées ultérieurement par le comité européen de la protection des données), p. 28, [https://ec.europa.eu/newsroom/article29/item-detail.cfm?item\\_id=612053](https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053) («Les responsables du traitement devraient procéder à des évaluations fréquentes des ensembles de données qu'ils traitent afin de vérifier s'il n'y a pas de biais, et élaborer des moyens de traiter tout élément préjudiciable, y compris toute dépendance excessive à l'égard des corrélations. Les systèmes qui vérifient les algorithmes et les examens réguliers de l'exactitude et de la pertinence de la prise de décision automatisée, y compris le profilage, sont d'autres mesures utiles. Les responsables du traitement devraient mettre en place des procédures et des mesures appropriées pour prévenir les erreurs, les inexacitudes ou la discrimination sur la base de données de catégories particulières. Ces mesures devraient être utilisées sur une base cyclique; non seulement au stade de la conception, mais aussi en permanence, car le profilage est appliqué aux individus»).

<sup>51</sup> CEPD, «Observations formelles du CEPD sur la proposition de règlement du Parlement européen et du Conseil relatif à la prévention de la diffusion de contenus à caractère terroriste en ligne», p. 8.

<sup>52</sup> Voir, dans le même esprit, avis du CEPD sur la proposition de dérogations aux fins de la lutte contre les abus sexuels commis contre des enfants en ligne, paragraphe 39 [https://edps.europa.eu/sites/edp/files/publication/20-11-10\\_opinion\\_combatting\\_child\\_abuse\\_en.pdf](https://edps.europa.eu/sites/edp/files/publication/20-11-10_opinion_combatting_child_abuse_en.pdf)

<sup>53</sup> CEPD, «Observations formelles du CEPD sur la proposition de règlement du Parlement européen et du Conseil relatif à la prévention de la diffusion de contenus à caractère terroriste en ligne», p. 9-10.

<sup>54</sup> Voir aussi COM (2020) 825 final, p. 5 («Cette proposition est sans préjudice du règlement (UE) 2016/679 (règlement général sur la protection des données) et des autres règles de l'Union relatives à la protection des données à caractère personnel et à la confidentialité des communications. Par exemple, les mesures concernant la publicité sur les plateformes en ligne complètent mais ne modifient pas les règles existantes sur le consentement et le droit d'opposition au traitement des données à caractère personnel. Elles imposent des obligations de transparence à l'égard des utilisateurs de plateformes en ligne, l'information fournie leur permettant également de faire usage de leurs droits en tant que personnes concernées. Elles permettent également aux autorités et aux chercheurs autorisés de contrôler la manière dont les publicités sont affichées et ciblées»).

<sup>55</sup> Estrada-Jiménez, José & Parra-Arnau, Javier & Rodríguez-Hoyos, Ana & Forné, Jordi. (2019). On the regulation of personal data distribution in online advertising platforms [sur la réglementation de la distribution de données à caractère personnel sur les plateformes de publicité en ligne]. Engineering Applications of Artificial Intelligence [applications d'ingénierie de l'intelligence artificielle]. 82. 13-29. 10.1016/j.engappai.2019.03.013.

<sup>56</sup> Voir aussi Parlement européen, «Résolution du Parlement européen du 20 octobre 2020 contenant des recommandations à la Commission concernant une législation sur les services numériques: adaptation des règles de droit commercial et civil pour les entités commerciales exerçant des activités en ligne (2020/2019(INL))», [https://www.europarl.europa.eu/doceo/document/TA-9-2020-0273\\_FR.html](https://www.europarl.europa.eu/doceo/document/TA-9-2020-0273_FR.html) paragraphe 18. En ce qui concerne l'article 22 de la proposition, le CEPD estime également qu'il convient de préciser les raisons pour lesquelles il existe une différence de traitement entre les personnes physiques et les personnes morales s'agissant de la communication des coordonnées bancaires [point c)], afin de garantir la traçabilité du professionnel.

<sup>57</sup> Le considérant (63) de la proposition elle-même mentionne «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».

<sup>58</sup> Parlement européen, «Résolution du Parlement européen du 20 octobre 2020 contenant des recommandations à la Commission concernant une législation sur les services numériques: adaptation des règles de droit commercial et civil pour les entités commerciales exerçant des activités en ligne (2020/2019(INL))» (2020/2019(INL)), paragraphe 15.

<sup>59</sup> Parlement européen, «Résolution du Parlement européen du 20 octobre 2020 contenant des recommandations à la Commission concernant une législation sur les services numériques: adaptation des règles de droit commercial et civil pour les entités commerciales exerçant des activités en ligne (2020/2019(INL))», paragraphe 17. Au minimum, le colégislateur devrait envisager d'introduire une exigence explicite, comme celle suggérée dans l'annexe d'une autre résolution du Parlement européen, visant à s'assurer que les personnes, par défaut, ne soient

---

pas suivies ou ne fassent pas l'objet d'un microciblage, et d'exiger que les personnes puissent opter elles-mêmes pour l'utilisation de données comportementales à des fins publicitaires, ainsi que pour l'affichage de messages publicitaires à caractère politique. Voir Parlement européen, «Résolution du Parlement européen du 20 octobre 2020 contenant des recommandations à la Commission sur la législation relative aux services numériques: améliorer le fonctionnement du marché unique, (2020/2018(INL))», p. 27 [https://www.europarl.europa.eu/doceo/document/TA-9-2020-0272\\_FR.pdf](https://www.europarl.europa.eu/doceo/document/TA-9-2020-0272_FR.pdf)

<sup>60</sup> Considérant (62) de la proposition.

<sup>61</sup> Voir Contrôleur européen de la protection des données, «Avis n° 3/2018 du CEPD sur la manipulation en ligne et les données à caractère personnel», 19 mars 2018, p. 9, [https://edps.europa.eu/sites/edp/files/publication/18-03-19\\_online\\_manipulation\\_fr.pdf](https://edps.europa.eu/sites/edp/files/publication/18-03-19_online_manipulation_fr.pdf) («*La manipulation se manifeste également par la présentation de contenu microciblé et géré, présenté comme étant le plus «pertinent» pour la personne, mais choisi dans l'objectif de maximiser les revenus de la plateforme. Cela ressemble aux «menus secrets» utilisés pour piloter les utilisateurs des sites de commerce électronique et les «dark patterns» utilisés pour les dissuader de prendre des décisions moins souhaitables du point de vue de la plateforme (comme le refus d'ajouter des objets supplémentaires, comme une assurance, à un panier d'achat)*»).

<sup>62</sup> Voir aussi point 67 ci-dessus (concernant la publicité en ligne).

<sup>63</sup> Article 31 de la proposition.

<sup>64</sup> Contrôleur européen de la protection des données, «A Preliminary Opinion on data protection and scientific research» [Avis préliminaire sur la protection des données et la recherche scientifique], 6 janvier 2020, [https://edps.europa.eu/sites/edp/files/publication/20-01-06\\_opinion\\_research\\_en.pdf](https://edps.europa.eu/sites/edp/files/publication/20-01-06_opinion_research_en.pdf).

<sup>65</sup> Contrôleur européen de la protection des données, «A Preliminary Opinion on data protection and scientific research» [Avis préliminaire sur la protection des données et la recherche scientifique], 6 janvier 2020, [https://edps.europa.eu/sites/edp/files/publication/20-01-06\\_opinion\\_research\\_en.pdf](https://edps.europa.eu/sites/edp/files/publication/20-01-06_opinion_research_en.pdf).

<sup>66</sup> 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: <https://ec.europa.eu/competition/publications/reports/kd0419345enn.pdf>. Voir également l'avis du CEPD relatif à la législation sur les marchés numériques.

<sup>67</sup> 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 n° 1673/2006/CE du Parlement européen et du Conseil. *JO L 316 du 14.11.2012, p. 12 à 33.*

<sup>68</sup> Voir <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 disponibles à l'adresse [https://edps.europa.eu/data-protection/our-work/subjects/big-data-digital-clearinghouse\\_fr](https://edps.europa.eu/data-protection/our-work/subjects/big-data-digital-clearinghouse_fr)