Mardi, 20 octobre 2020

P9_TA(2020)0274

Législation sur les services numériques et questions liées aux droits fondamentaux

Résolution du Parlement européen du 20 octobre 2020 sur la législation relative aux services numériques et les questions liées aux droits fondamentaux (2020/2022(INI))

(2021/C 404/03)

Le Parlement européen,

— vu le traité sur l'Union européenne (traité UE), et notamment son article 2,

— vu le traité sur le fonctionnement de l'Union européenne (traité FUE), et notamment ses articles 16 et 114,

— vu la charte des droits fondamentaux de l'Union européenne, et notamment ses articles 6, 7, 8, 11, 13, 21, 22, 23, 24, 26, 38 et 47,

— vu la directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur («directive sur le commerce électronique») ([1]),

— 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», RGPD) ([2]),

— vu la directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques («directive relative à la vie privée et aux communications électroniques») ([3]),

— vu la directive (UE) 2018/1808 du Parlement européen et du Conseil du 14 novembre 2018 modifiant la directive 2010/13/UE visant à la coordination de certaines dispositions législatives, réglementaires et administratives des États membres relatives à la fourniture de services de médias audiovisuels (directive «Services de médias audiovisuels»), compte tenu de l'évolution des réalités du marché ([4]);

— vu la directive (UE) 2019/790 du Parlement européen et du Conseil du 17 avril 2019 sur le droit d'auteur et les droits voisins dans le marché unique numérique et modifiant les directives 96/9/CE et 2001/29/CE («directive sur le droit d'auteur») ([5])

— vu la recommandation de la Commission (UE) 2018/334 du 1er mars 2018 sur les mesures destinées à lutter, de manière efficace, contre les contenus illicites en ligne ([6]);

— vu le rapport d'Europol sur l'évaluation de la menace que représente la criminalité organisée sur l'internet (IOCTA) du 18 septembre 2018,

— vu la jurisprudence de la Cour de justice de l'Union européenne en la matière,

— vu l'article 54 de son règlement intérieur,

— vu les avis de la commission du marché intérieur et de la protection des consommateurs et de la commission de la culture et de l'éducation,

— vu le rapport de la commission des libertés civiles, de la justice et des affaires intérieures (A9-0172/2020),

([1]) JO L 178 du 17.7.2000, p. 1.
([2]) JO L 119 du 4.5.2016, p. 1.
([3]) JO L 201 du 31.7.2002, p. 37.
([4]) JO L 303 du 28.11.2018, p. 69.
([5]) JO L 130 du 17.5.2019, p. 92.
([6]) JO L 63 du 6.3.2018, p. 50.

Mardi, 20 octobre 2020

A. considérant que les droits fondamentaux, tels que la protection de la vie privée et des données à caractère personnel, le principe de non-discrimination, ainsi que la liberté d'expression et d'information doivent être ancrés au cœur d'une politique européenne efficace et durable en matière de services numériques; considérant que ces droits doivent apparaître à la fois dans la lettre de la loi et dans l'esprit de leur mise en œuvre;

B. considérant que les types de services numériques et les rôles des fournisseurs de services numériques ont fortement évolué depuis l'adoption de la directive sur le commerce électronique il y a 20 ans;

C. considérant que la confiance des utilisateurs ne peut être gagnée que par l'intermédiaire de services numériques qui respectent leurs droits fondamentaux, ce qui permet de garantir à la fois le recours à ces services, ainsi qu'un avantage concurrentiel et des modèles économiques stables pour les entreprises;

D. considérant que les règles en matière de protection des données applicables à tous les fournisseurs de services numériques sur le territoire de l'Union européenne ont été récemment actualisées et harmonisées dans l'ensemble de l'Union par le règlement général sur la protection des données (RGPD); considérant que les règles relatives à la protection de la vie privée dans le secteur des communications électroniques, qui concernent une partie des services numériques, sont couvertes par la directive relative à la vie privée et aux communications électroniques et sont en cours de révision;

E. considérant que la quantité de contenus de tout genre créés et partagés par les utilisateurs et de services fournis par l'intermédiaire de plateformes en ligne, y compris de services d'informatique en nuage, a augmenté de manière exponentielle à un rythme sans précédent grâce aux progrès technologiques; considérant que cela inclut des contenus illicites, tels que des images pédopornographiques en ligne, et des contenus licites, mais préjudiciables pour la société et la démocratie, par exemple la désinformation quant aux remèdes contre la COVID-19;

F. considérant que les discours de haine et la désinformation en ligne se sont multipliés ces dernières années, car les acteurs et les individus perturbateurs utilisent les plateformes en ligne pour accroître la polarisation, ce qui sert des fins politiques; considérant que les femmes, les personnes de couleur, les personnes appartenant ou perçues comme appartenant à des minorités ethniques ou linguistiques et les personnes LGBTIQ sont souvent la cible de discours de haine discriminatoires, d'intimidations, de menaces et d'accusations en ligne;

G. considérant que cette tendance a été favorisée par des plateformes en ligne dont le modèle économique repose sur la collecte et l'analyse des données des utilisateurs en vue de générer davantage de trafic et de «clics», et donc davantage de données de profilage et de profits; considérant que cela conduit à une multiplication des contenus sensationnalistes; considérant que les discours de haine et la désinformation nuisent à l'intérêt public en discréditant les discours publics respectueux et honnêtes, et menacent la sécurité publique en ce sens qu'ils peuvent engendrer de la violence dans le monde réel; considérant que la lutte contre ce type de contenus est essentielle pour garantir le respect des droits fondamentaux et défendre l'état de droit et la démocratie au sein de l'Union européenne;

H. considérant que les médias sociaux et les autres plateformes de distribution de contenus ont recours à des techniques de profilage pour orienter et diffuser leurs contenus, ainsi que des publicités; considérant que les données collectées à partir des traces numériques laissées par les individus peuvent être exploitées de manière à déduire des informations très personnelles avec un grand degré de précision, en particulier lorsque ces données sont combinées avec d'autres ensembles de données; considérant que les scandales Facebook et Cambridge Analytica ont illustré les risques associés aux opérations de traitement de données réalisées de manière opaque par les plateformes en ligne, en révélant que certains électeurs avaient été microciblés par des publicités politiques et, parfois, par une désinformation orientée;

I. considérant que les algorithmes automatisés qui décident de la manière de traiter, de hiérarchiser, de diffuser et de supprimer les contenus tiers disponibles sur les plateformes en ligne, y compris pendant les campagnes politiques et électorales, reproduisent souvent des schémas discriminatoires existants au sein de la société, et créent ainsi un risque élevé de discrimination envers les personnes déjà concernées; considérant que l'utilisation généralisée d'algorithmes dans la suppression et le blocage de contenus soulève également des inquiétudes quant au respect de l'état de droit et des interrogations en matière de légalité, de légitimité et de proportionnalité;

J. considérant qu'un petit nombre de fournisseurs de services, pour la plupart non européens, disposent d'une part de marché importante et d'une certaine influence sur les droits et les libertés des individus, sur nos sociétés et sur nos démocraties en contrôlant la manière dont les informations, les services et les produits sont présentés, ce qui a une

incidence considérable sur le fonctionnement des États membres et sur leurs citoyens; considérant que les décisions de ces plateformes peuvent avoir de lourdes conséquences sur la liberté d'expression et d'information, ainsi que sur la liberté et le pluralisme des médias;

K. considérant que l'approche législative contre les contenus illicites en ligne dans l'Union a, jusqu'à présent, principalement consisté en une coopération volontaire et en des retraits imposés par décision judiciaire, mais que de plus en plus d'États membres légifèrent à l'échelle nationale pour lutter contre les contenus illicites de manière non harmonisée; considérant que des dispositions visant à lutter contre certains types de contenus illicites ont été incluses dans la législation sectorielle récemment adoptée à l'échelle de l'Union;

L. considérant qu'une approche fondée uniquement sur l'autorégulation des plateformes ne permet pas d'offrir suffisamment de transparence, de responsabilité et de contrôle; considérant qu'une telle approche n'apporte pas non plus d'informations appropriées aux autorités publiques, à la société civile et aux utilisateurs sur la manière dont les plateformes luttent contre les contenus et activités illicites ainsi que contre les contenus qui enfreignent leurs conditions d'utilisation, ni sur la manière dont elles éditent généralement les contenus;

M. considérant qu'une telle approche ne garantit pas nécessairement le respect des droits fondamentaux et crée une situation dans laquelle les responsabilités juridiques sont en partie déléguées à des parties privées, ce qui risque d'empiéter sur la liberté d'expression;

N. considérant que la surveillance et la supervision réglementaires sont organisées de manière sectorielle au sein de l'Union; considérant qu'une coordination plus poussée et plus complète entre les différents organes de surveillance de l'Union européenne serait bénéfique;

O. considérant que le manque de données publiques solides et comparables sur la prévalence des contenus illicites et préjudiciables en ligne, sur les signalements et les suppressions de ces contenus, qu'elles soient imposées par décision judiciaire ou qu'elles relèvent d'une démarche d'autorégulation, ainsi que sur le suivi assuré par les autorités compétentes provoque un manque de responsabilité et de transparence, tant dans le secteur privé que dans le secteur public; considérant que l'on dispose de trop peu d'informations sur les algorithmes dont se servent les plateformes et les sites ainsi que sur la manière dont les plateformes traitent les suppressions erronées de contenus;

P. considérant que l'exploitation sexuelle des enfants en ligne alimente une forme de contenus illicites rendus plus accessibles par les évolutions de la technologie; considérant que la grande quantité de contenus pédopornographiques qui circulent en ligne pose de graves difficultés en matière de repérage, d'enquête et surtout d'identification des victimes; considérant que, d'après Europol, le National Center for Missing and Exploited Children («Centre national pour les enfants disparus ou exploités») des États-Unis a enregistré l'année dernière une hausse de 106 % des signalements de partage en ligne de contenus pédopornographiques;

Q. considérant que la jurisprudence de la Cour de justice de l'Union européenne impose la suppression des contenus sur décision judiciaire émise par une juridiction d'un État membre; considérant que les hébergeurs peuvent avoir recours à des outils et à des technologies de recherche automatisée afin de détecter et de supprimer les contenus équivalents à un autre qui a déjà été déclaré illicite, mais ne devraient pas être tenus à une obligation générale de surveiller les informations qu'ils stockent, ni de rechercher activement des faits ou des circonstances révélant des activités illicites, conformément à l'article 15, paragraphe 1, de la directive 2000/31/CE;

R. considérant qu'une identification électronique fiable est un moyen élémentaire de garantir un accès sécurisé aux services numériques et d'effectuer des transactions électroniques d'une manière plus sûre; considérant qu'à l'heure actuelle, seuls 15 États membres ont notifié à la Commission leur schéma d'identification électronique pour une reconnaissance transfrontalière dans le cadre du règlement (UE) nº 910/2014 («le règlement eIDAS») ([7]);

S. considérant que l'internet et les plateformes en ligne restent un terrain essentiel pour les groupes terroristes, qui les utilisent comme outils de propagande, de recrutement et de promotion de leurs actions;

([7]) Règlement (UE) nº 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE (JO L 257 du 28.8.2014, p. 73).

Mardi, 20 octobre 2020

1. estime qu'un marché unique numérique opérationnel présente des avantages économiques et sociétaux évidents pour l'Union européenne et ses États membres; se réjouit de ces avantages, en particulier de l'amélioration de l'accès à l'information et du renforcement de la liberté d'expression; souligne l'obligation importante de veiller au caractère équitable de l'écosystème numérique, afin de respecter les droits fondamentaux consacrés par les traités et la charte des droits fondamentaux de l'Union européenne, en particulier la liberté d'expression et d'information, la non-discrimination, la liberté et le pluralisme des médias, le respect de la vie privée et la protection des données, et de garantir la sécurité en ligne; insiste sur la nécessité de limiter au strict nécessaire les interventions législatives et réglementaires dans le marché unique numérique qui visent à assurer que cette obligation est suivie; rappelle que les mécanismes de suppression des contenus activés en dehors des garanties d'une procédure régulière sont contraires à l'article 10 de la Convention européenne des droits de l'homme;

2. demande instamment à la Commission d'adopter une approche réglementaire sur mesure pour faire face aux différences persistantes entre monde hors ligne et monde en ligne, ainsi qu'à toutes les difficultés soulevées par la diversité des acteurs et des services proposés en ligne; considère essentiel, à cet égard, d'appliquer des approches réglementaires différentes aux contenus illicites et licites; souligne qu'il faut lutter contre les contenus illicites en ligne et les infractions facilitées par l'internet avec autant de rigueur, en suivant les mêmes principes juridiques et en apportant les mêmes garanties aux citoyens que dans la lutte contre les contenus illicites et les comportements illégaux hors ligne; rappelle que la gestion des contenus est encadrée juridiquement par la directive sur le commerce électronique applicable aux services en ligne au sein du marché intérieur;

3. juge nécessaire la suppression rapide et systématique des contenus illicites, afin de lutter contre les infractions et les violations des droits fondamentaux; considère que des codes de conduite volontaires ne constituent qu'une solution partielle;

4. invite les fournisseurs de services numériques à supprimer les contenus de manière diligente, mesurée et non discriminatoire, dans le respect, en toutes circonstances, des droits fondamentaux des utilisateurs, et à tenir compte de l'importance capitale de la liberté d'expression et d'information dans une société ouverte et démocratique afin d'éviter le retrait de contenus licites; demande aux fournisseurs de services numériques qui souhaitent, de leur propre initiative, restreindre certains contenus licites de leurs utilisateurs d'envisager la possibilité de signaler les contenus concernés plutôt que de les supprimer, afin de laisser aux utilisateurs une chance de choisir d'accéder à ces contenus en toute responsabilité;

5. estime que toute mesure de suppression des contenus juridiquement imposée par la législation sur les services numériques devrait uniquement s'appliquer aux contenus illicites tels que définis dans les législations européennes ou nationales; croit que ces textes législatifs ne devraient pas comprendre de termes ou concepts imprécis, car cela entraînerait de l'insécurité juridique pour les plateformes en ligne et mettrait en péril les droits fondamentaux et la liberté d'expression;

6. constate néanmoins que l'écosystème numérique actuel encourage les comportements problématiques, tels que le microciblage fondé sur des caractéristiques faisant état de vulnérabilités physiques ou psychologiques ou la diffusion de discours de haine, de contenus racistes et de désinformation, mais fait également surgir de nouvelles questions comme les violations organisées des conditions d'utilisation de plusieurs plateformes et la présence d'algorithmes créant de faux profils ou manipulant les contenus en ligne; relève avec inquiétude que certains modèles commerciaux s'appuient sur la diffusion de contenus sensationnalistes et clivants, afin d'augmenter le temps que les utilisateurs passent devant leur écran et ainsi de maximiser les profits des plateformes en ligne; souligne les effets néfastes de ces modèles commerciaux pour les droits fondamentaux des individus et la société dans son ensemble; réclame davantage de transparence dans les politiques de monétisation des plateformes en ligne;

7. souligne par conséquent qu'il convient d'endiguer la diffusion de ces contenus préjudiciables; est fermement convaincu que les compétences relevant de l'éducation aux médias, le contrôle de l'utilisateur sur le contenu qui lui est présenté et l'accès public à des contenus et à une éducation de qualité revêtent à cet égard une importance capitale; salue donc l'initiative de la Commission de créer un Observatoire européen des médias numériques pour soutenir les services indépendants de vérification des faits, accroître les connaissances du public sur la désinformation en ligne et soutenir les autorités publiques chargées de surveiller les médias numériques;

8. invite la Commission et les États membres à soutenir les médias publics comme indépendants, les initiatives pédagogiques en matière d'éducation aux médias et les campagnes de sensibilisation ciblées au sein de la société civile; invite à porter davantage d'attention sur les contenus préjudiciables dans le contexte de l'utilisation de l'internet par des mineurs, notamment en ce qui concerne leur exposition à la cyberintimidation, au harcèlement sexuel, à la pornographie, à la violence et à l'automutilation;

9. remarque que, étant donné que les activités en ligne d'une personne permettent d'acquérir des connaissances approfondies sur sa personnalité, ce qui rend possible sa manipulation, la collecte générale et systématique de données à caractère personnel concernant chaque utilisation d'un service numérique empiète de façon disproportionnée sur le droit à la vie privée et sur la protection des données à caractère personnel; souligne en particulier que la publicité microciblée ou comportementale et l'évaluation des personnes peuvent avoir des conséquences négatives, en particulier sur les mineurs et les autres groupes vulnérables, parce qu'elles constituent une intrusion dans la vie privée des individus et soulèvent des questions quant à la collecte et à l'utilisation des données servant à personnaliser la publicité, à proposer des produits ou des services, ou à fixer des prix; réaffirme que le RGPD protège le droit des utilisateurs de ne pas faire l'objet d'un suivi généralisé lorsqu'ils utilisent des services numériques; déclare que ce droit devrait être correctement appliqué dans l'ensemble de l'Union; note que la Commission a proposé de soumettre l'édition ciblée de contenus à une décision d'acceptation dans sa proposition de nouveau règlement concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques (2017/0003(COD));

10. estime que la publicité politique trompeuse ou obscure relève d'une catégorie spéciale de menace en ligne parce qu'elle influence les mécanismes fondamentaux qui permettent le fonctionnement de notre société démocratique, notamment lorsqu'un tel contenu est parrainé par des acteurs tiers, parfois étrangers; insiste sur le fait que, lorsque le profilage est déployé à une échelle permettant au microciblage politique de manipuler les comportements de vote, il peut gravement porter atteinte aux fondements de la démocratie; invite donc les fournisseurs de services numériques à prendre les mesures nécessaires en vue de la détection et du signalement des contenus mis en ligne par des robots sur les réseaux sociaux; espère que la Commission présentera des lignes directrices sur l'utilisation de ces technologies numériques visant à convaincre dans le cadre de campagnes électorales et de la publicité politique; demande, à cet égard, l'établissement d'obligations strictes de transparence pour l'affichage de publicité politique payante;

11. juge nécessaire la suppression systématique et sans délai des contenus illicites afin de réagir aux infractions, notamment lorsqu'elles touchent des enfants ou relèvent de contenus terroristes, et aux violations des droits fondamentaux, tout en mettant en place les garanties nécessaires, telles que la transparence de la procédure, le droit de recours et l'accès à un recours judiciaire efficace; considère que les codes de conduite volontaires et les conditions d'utilisation normalisées ne sont pas correctement appliqués et ne constituent qu'une solution partielle au problème; souligne que la responsabilité de veiller au respect de la législation, de décider de la légalité d'activités en ligne et d'ordonner aux fournisseurs de services d'hébergement de retirer des contenus illégaux ou d'empêcher d'y avoir accès devrait incomber en dernière instance à des autorités compétentes indépendantes;

12. remarque qu'il est facile d'établir le caractère illicite de certains types de contenu, mais que la décision est plus difficile pour d'autres types de contenu qu'il faut replacer dans leur contexte; met en garde quant à l'incapacité des outils automatisés actuels à réaliser des analyses critiques et à saisir correctement l'importance du contexte pour certains contenus, ce qui pourrait entraîner des suppressions inutiles, restreindre la liberté d'expression et l'accès à diverses informations, notamment lorsqu'il s'agit d'opinions politiques, et mener à une forme de censure; souligne qu'un examen humain des rapports automatisés effectué par les fournisseurs de services ou leurs contractants ne suffit pas à résoudre ce problème, surtout lorsque cet examen est externalisé auprès du personnel d'entreprises privées, qui manque d'indépendance, de qualifications et de responsabilité;

13. relève avec inquiétude que les contenus illicites en ligne peuvent facilement se multiplier rapidement, ce qui amplifie considérablement leur incidence négative sur une très courte période; croit toutefois que la législation sur les services numériques ne devrait pas prévoir d'obligation pour les fournisseurs de services d'hébergement ou les autres intermédiaires techniques d'utiliser des outils automatisés pour la modération des contenus;

14. rappelle que les contenus illicites en ligne devraient non seulement être supprimés des plateformes en ligne, mais également faire l'objet d'un suivi par les services répressifs et judiciaires lorsqu'ils découlent d'activités illégales; invite la Commission à envisager d'obliger les plateformes en ligne à informer l'autorité compétente de toute infraction grave dès qu'ils prennent connaissance d'une telle infraction; pense à cet égard que dans certains États membres, ce n'est pas tant l'existence d'affaires non résolues que celle d'affaires jamais ouvertes qui constitue un problème essentiel; demande l'élimination des obstacles entravant le dépôt de plaintes auprès des autorités compétentes; est convaincu que la coopération entre les fournisseurs de services et les autorités nationales compétentes, ainsi que la coopération transfrontalière entre les autorités nationales compétentes, devrait être renforcée et s'appuyer sur les principes de nécessité et de proportionnalité, étant donné que l'internet ne connaît pas de frontières et que les contenus illicites en ligne se diffusent rapidement; souligne à cet égard la nécessité de respecter l'ordre juridique de l'Union européenne et les principes établis de coopération

transfrontalière et de confiance mutuelle; invite les États membres à doter leurs services répressifs et leurs autorités judiciaires de l'expertise, des ressources et des outils nécessaires pour leur permettre de traiter de manière efficace et efficiente le nombre croissant d'affaires relatives à la présence de contenus illicites en ligne; recommande la mise en place d'un mécanisme de règlement des litiges en vue de la suppression des contenus, ainsi que l'élargissement de l'accès à la justice en matière de services numériques;

15. souligne qu'un contenu spécifique peut être jugé illicite dans un État membre, mais relever de la liberté d'expression dans un autre; souligne que pour protéger la liberté d'expression, prévenir les conflits de lois, éviter un recours injustifié et inutile au géoblocage et harmoniser le marché unique numérique, les fournisseurs de services d'hébergement ne devraient pas être contraints de supprimer des informations ou l'accès à des informations lorsque celles-ci sont légales dans l'État membre où ils sont établis ou dans celui où leur représentant légal désigné réside ou est établi; rappelle que les autorités nationales ne peuvent faire appliquer des injonctions de suppression que si elles sont émises par des autorités compétentes indépendantes à l'intention de fournisseurs de services établis sur leur territoire; estime nécessaire de renforcer les mécanismes de coopération entre les États membres, avec le soutien de la Commission et des agences de l'Union européenne concernées; demande l'établissement d'un dialogue structuré entre les États membres afin de déterminer les risques posés par chaque type de contenu et de détecter toute différence éventuelle entre États membres dans l'évaluation de ces risques;

16. souligne que les contenus illicites devraient être supprimés à l'endroit où ils sont hébergés, et que les simples intermédiaires relayant ces contenus ne devraient pas être tenus de bloquer l'accès à ceux-ci;

17. se déclare fermement convaincu que le cadre juridique actuel de l'Union concernant les services numériques devrait être modernisé, afin de répondre aux questions soulevées par les divergences entre les États membres face aux nouvelles technologies, en ce qui concerne par exemple la prévalence du profilage et des prises de décision au moyen d'algorithmes dans tous les aspects du quotidien, ainsi que de garantir la clarté juridique et le respect des droits fondamentaux, notamment la liberté d'expression et le droit au respect de la vie privée, d'une manière susceptible de résister à l'épreuve du temps, étant donné les évolutions rapides de la technologie;

18. salue la volonté de la Commission d'introduire une approche harmonisée concernant les obligations imposées aux fournisseurs de services numériques, y compris les intermédiaires en ligne, afin de prévenir la fragmentation du marché intérieur et l'application disparate de la réglementation; invite donc la Commission à proposer les solutions les plus efficaces et efficientes pour le marché intérieur dans son ensemble, tout en évitant de créer de nouvelles formalités administratives inutiles et en gardant le marché unique numérique ouvert, équitable, sûr et concurrentiel pour tous ses participants; souligne que le régime de responsabilité pour les fournisseurs de services numériques doit être proportionné, ne pas désavantager les petits et moyens fournisseurs et ne pas freiner l'innovation et l'accès à l'information de manière injustifiée;

19. estime qu'une réforme en ce sens devrait pleinement respecter le droit européen existant, s'appuyer sur ses fondements solides, en particulier le RGPD et la directive relative à la vie privée et aux communications électroniques, en cours de révision, et respecter la primauté d'autres instruments sectoriels tels que la directive «Services de médias audiovisuels»; souligne que la modernisation des règles en matière de commerce électronique peut avoir une incidence sur les droits fondamentaux; demande donc instamment à la Commission d'être extrêmement vigilante dans son approche et de tenir compte également des normes internationales relatives aux droits de l'homme lors de la révision de la réglementation;

20. souligne que la capacité pratique des utilisateurs individuels à naviguer dans les écosystèmes de données et à comprendre leur complexité est extrêmement limitée, tout comme leur aptitude à déterminer si les informations qu'ils reçoivent et les services qu'ils utilisent sont mis à leur disposition selon les mêmes conditions que les autres utilisateurs; prie donc la Commission de placer les principes de transparence et de non-discrimination au cœur de la législation sur les services numériques;

21. précise que la législation sur les services numériques doit viser à assurer un niveau élevé de transparence en ce qui concerne le fonctionnement des services en ligne et un environnement numérique exempt de discrimination; souligne qu'outre le cadre réglementaire strict qui protège actuellement la vie privée et les données à caractère personnel, il doit incomber aux plateformes en ligne de veiller à l'utilisation légitime des algorithmes; demande donc à la Commission d'élaborer un régime fondé sur la directive sur le commerce électronique qui encadre clairement la responsabilité des fournisseurs de services de gérer les risques auxquels leurs utilisateurs sont confrontés et de protéger les droits de ceux-ci; prie la Commission d'instaurer une obligation de transparence et d'explicabilité des algorithmes, de prévoir des sanctions visant à assurer le respect de cette obligation, de permettre une intervention humaine et de prendre d'autres mesures, telles que des audits indépendants annuels et des tests de résistance spécifiques visant à faciliter et à assurer la conformité;

22. souligne que certains fournisseurs de services numériques ont réussi à identifier sans ambiguïté leurs utilisateurs de manière équivalente aux services hors ligne; constate que, lors de l'inscription à un service, les plateformes en ligne collectent des données à caractère personnel superflues, telles que le numéro de téléphone mobile, souvent parce qu'elles utilisent des systèmes d'authentification unique; souligne que le RGPD décrit clairement le principe de minimisation des données, limitant ainsi la collecte des données à celles strictement nécessaires à l'objectif poursuivi; recommande que les plateformes en ligne qui assurent un service d'authentification unique occupant une position dominante sur le marché soient tenues de proposer au moins un système d'identité ouvert, s'appuyant sur un cadre non exclusif, décentralisé et interopérable;

23. souligne que lorsqu'un certain type d'identification officielle est nécessaire hors ligne, il est indispensable de créer un système d'identification électronique sécurisé équivalent; est d'avis que l'identification en ligne peut être améliorée en appliquant l'interopérabilité transfrontalière des identifications électroniques prévue par le règlement eIDAS dans toute l'Union européenne; invite la Commission à envisager de créer un système européen commun d'authentification permettant d'éviter les systèmes privés d'authentification unique, et à imposer aux services numériques une obligation de proposer systématiquement comme possibilité par défaut une identification manuelle; souligne qu'il convient de développer ce service de manière à ce que la collecte de données identifiables enregistrées par le prestataire du service d'authentification soit techniquement impossible et que les données recueillies soient limitées au strict minimum; recommande donc à la Commission d'étudier également la mise au point d'un système de vérification pour les utilisateurs de services numériques afin de garantir la protection des données à caractère personnel et la vérification de l'âge, en particulier pour les mineurs, système qui ne devrait pas être utilisé à des fins commerciales, ni pour suivre les utilisateurs entre les sites; souligne que ces systèmes d'authentification et de vérification ne devraient s'appliquer qu'aux services numériques qui nécessitent une identification personnelle, une authentification ou une vérification de l'âge; rappelle que les États membres et les institutions de l'Union doivent veiller à la sécurité et à la transparence des systèmes d'authentification électronique, au fait qu'ils traitent uniquement les données nécessaires à l'identification de l'utilisateur et qu'ils ne sont utilisés qu'à des fins légitimes et non commerciales, ni pour restreindre l'accès général à l'internet ou suivre les utilisateurs entre les sites;

24. juge indispensable d'harmoniser et de clarifier intégralement les règles au niveau européen sur la responsabilité, en vue de garantir le respect des droits fondamentaux et les libertés des utilisateurs dans l'ensemble de l'Union; estime que de telles règles devraient maintenir les exemptions de responsabilité pour les intermédiaires n'ayant pas effectivement connaissance des activités ou informations illicites sur leurs plateformes; se déclare préoccupé par la fragmentation croissante des règles et par la diminution du niveau de protection des droits fondamentaux dans l'Union entraînées par l'adoption récente de législations nationales visant à lutter contre les discours de haine et la désinformation;

25. demande donc des propositions législatives qui maintiennent l'ouverture et la compétitivité du marché unique numérique, en harmonisant les exigences imposées aux fournisseurs de services numériques en matière de procédures et de garanties procédurales efficaces, cohérentes, transparentes et équitables pour traiter les contenus illicites en ligne, conformément à la législation nationale et européenne, y compris en mettant en place une procédure harmonisée de notification et d'action;

26. croit à cet égard qu'il est primordial pour les plateformes en ligne de disposer de règles, d'obligations et de garanties claires en matière de responsabilité vis-à-vis des contenus de tiers; propose la mise en place d'un cadre réglementaire commun, afin de repérer et de supprimer les contenus illicites de manière efficace;

27. insiste sur l'importance de compléter les règles sur les procédures de notification et d'action par l'obligation pour les plateformes de prendre des mesures spécifiques, proportionnées à leur portée d'action et à leurs capacités techniques et opérationnelles, pour lutter efficacement contre l'émergence de contenus illicites sur leur infrastructure; note dès lors que, lorsque cela est technologiquement faisable, sur demande dûment motivée des autorités publiques indépendantes compétentes, et en tenant pleinement compte du contexte spécifique du contenu, il peut être demandé aux fournisseurs de services numériques de rechercher régulièrement certains contenus déjà déclarés illicites par un tribunal, pour autant que la surveillance et la recherche des informations concernées par une telle injonction sont limitées à des informations véhiculant un message dont le contenu demeure, en substance, inchangé par rapport à celui ayant donné lieu au constat d'illicéité et comportant les éléments spécifiés dans l'injonction, qui, conformément à l'arrêt de la Cour de justice du 3 octobre 2019 dans l'affaire C-18/18 ([8]), sont à ce point identiques ou équivalents qu'il n'y a pas lieu de contraindre l'hébergeur à procéder à une appréciation autonome de ce contenu;

([8]) Arrêt de la Cour de justice du 3 octobre 2019, Eva Glawischnig-Piesczek/Facebook Ireland Limited, C-18/18, ECLI:EU:C:2019:821.

28. estime que le choix des initiatives concrètes devrait être laissé aux plateformes; se déclare favorable à une approche équilibrée et fondée sur un dialogue avec les parties prenantes et une évaluation des risques encourus par les plateformes, ainsi qu'à une chaîne de responsabilité claire, afin de ne pas faire peser des charges réglementaires superflues sur les plateformes ni de restreindre de manière inutile ou disproportionnée les droits fondamentaux, en particulier la liberté d'expression, l'accès à l'information, notamment lorsqu'il s'agit d'opinions politiques, et le droit au respect de la vie privée; souligne que certains devoirs peuvent être précisés par la législation sectorielle; signale que toute mesure mise en place à cette fin ne peut constituer une obligation générale de surveillance, ni en droit ni en fait;

29. souligne la nécessité de mettre en place des garanties appropriées et des obligations de traitement équitable, notamment en exigeant une surveillance et une vérification humaines, ainsi que des procédures de contre-signalement, afin de permettre aux propriétaires des contenus et à ceux qui les ont mis en ligne de défendre leurs droits comme il se doit et en temps voulu, mais aussi de veiller à la légalité, à la précision et au bien-fondé des décisions de suppression ou de blocage, à la protection des utilisateurs ainsi qu'au respect des droits fondamentaux; insiste pour que les personnes qui adressent systématiquement et de façon répétée des notifications injustifiées ou abusives soient sanctionnées; rappelle qu'un recours juridictionnel effectif, outre les procédures de contre-signalement et les règlements extrajudiciaires effectués par les plateformes conformément à leur système interne de réclamations, devrait toujours rester accessible afin de respecter le droit à un recours effectif;

30. approuve la conservation du cadre actuel régissant la responsabilité limitée relative aux contenus ainsi que le principe du pays d'origine, mais estime qu'il est essentiel d'améliorer la coordination des demandes de suppression entre les autorités nationales compétentes; souligne que les contenus illicites doivent être supprimés là où ils sont hébergés; insiste pour que ces demandes fassent l'objet de garanties juridiques, afin d'éviter les abus et d'assurer le plein respect des droits fondamentaux; souligne que les demandes de suppression émises par les autorités compétentes devraient être spécifiques et indiquer clairement le fondement juridique de la suppression; souligne qu'un mécanisme efficace de surveillance et d'application, comprenant des sanctions proportionnées et tenant compte des capacités techniques et opérationnelles, devrait s'appliquer aux fournisseurs de services qui n'accèdent pas aux demandes légitimes;

31. rappelle que les fournisseurs de services numériques ne doivent pas être légalement tenus de conserver de données à caractère personnel de leurs utilisateurs ou abonnés à des fins répressives, sauf si la conservation ciblée est ordonnée par une autorité compétente indépendante, dans le plein respect du droit de l'Union et de la jurisprudence de la Cour de justice de l'Union européenne; rappelle également que la conservation de données dans ce cadre devrait se limiter au strict nécessaire en ce qui concerne les catégories de données à conserver, les personnes et les moyens de communication concernés ainsi que la période de conservation retenue;

32. pense que, afin de protéger les droits fondamentaux, la législation sur les services numériques devrait introduire des règles visant à garantir que les conditions d'utilisation des fournisseurs de services numériques sont claires, transparentes, équitables et facilement accessibles aux utilisateurs; regrette que les conditions d'utilisation de certaines plateformes de contenu obligent les agents des services répressifs à utiliser des comptes personnels pour enquêter sur certaines plaintes, ce qui entrave les enquêtes et met en péril la sécurité personnelle; souhaite une coordination plus efficace entre les États membres en ce qui concerne le suivi de l'application de la législation en matière de contenus illicites signalés; rappelle que toute demande de suppression adressée par une autorité compétente indépendante doit être fondée sur le droit et non sur les conditions d'utilisation des fournisseurs de services;

33. invite la Commission à s'assurer que les utilisateurs ont accès à un contenu en ligne diversifié et de qualité, afin de les aider à devenir des citoyens suffisamment informés; souhaite que la législation sur les services numériques veille à ce que les contenus médiatiques de qualité soient aisément accessibles et trouvables sur les plateformes tierces, et à ce que les suppressions de contenus respectent les normes en matière de droits de l'homme et se limitent au contenu indubitablement illicite ou jugé illicite par une autorité compétente indépendante; souligne que les contenus légaux ne devraient pouvoir faire l'objet d'aucune obligation juridique de suppression ou de blocage;

34. est favorable à un dialogue renforcé entre les États membres, les autorités compétentes et les parties prenantes concernées dans le but de mettre au point des démarches non contraignantes, comme le code européen de bonnes pratiques contre la désinformation, de les évaluer et de les améliorer, afin de mieux lutter contre la désinformation et les autres catégories de contenus licites; souhaite que la Commission publie des lignes directrices qui prévoient des règles obligeant à davantage de transparence concernant la modération des contenus et les pratiques vis-à-vis de la publicité, sous forme d'un instrument d'accompagnement spécifique de la législation sur les services numériques, afin de veiller à ce que la suppression et le blocage de contenus licites effectués sur la base des conditions d'utilisation se limitent au strict nécessaire;

demande en outre à la Commission d'établir un cadre qui interdise aux plateformes d'exercer un deuxième niveau de contrôle sur les contenus mis à disposition sous la responsabilité d'un fournisseur de services médiatiques et qui sont soumis à des normes et à une surveillance spécifiques;

35. souligne par ailleurs que les utilisateurs devraient disposer d'un choix et d'un contrôle plus vastes quant aux contenus qu'ils consultent, ce qui implique des options sur la manière dont les contenus sont organisés pour eux et la possibilité de refuser toute organisation des contenus; est fermement convaincu que la conception et la performance de systèmes de recommandation devraient tenir compte de la convivialité d'utilisation et être soumises à une obligation de transparence totale;

36. estime que l'obligation de rendre des comptes, tant pour le secteur privé que pour le secteur public, et l'élaboration de mesures fondées sur des éléments factuels requièrent des données solides sur la prévalence des contenus et des activités illicites en ligne, les mesures prises dans ce domaine et la manière dont les contenus sont supprimés, ainsi que sur les algorithmes d'organisation de contenus des plateformes en ligne;

37. demande à cet égard que les plateformes soient soumises à une obligation de publier des rapports annuels exhaustifs et approfondis, qui soit proportionnée à leur portée d'action et à leurs capacités opérationnelles, plus précisément sur leurs procédures de modération des contenus, y compris des informations sur les mesures adoptées contre les activités illicites en ligne et des données normalisées sur la quantité de contenus supprimés, les motifs et les bases juridiques sous-jacents, le type et la justification des demandes de suppression reçues, le nombre de demandes dont l'exécution a été refusée et les motifs de ces refus; précise qu'un rapport portant sur les activités d'une année donnée devrait être publié avant la fin du premier trimestre de l'année suivante;

38. appelle également de ses vœux une obligation pour les autorités nationales de publier des rapports annuels comprenant des données normalisées sur le nombre de demandes de suppression et leurs bases juridiques, sur le nombre de demandes de suppression ayant fait l'objet de recours administratifs ou judiciaires, sur l'issue de ces procédures, en mentionnant celles concernant des contenus ou activités accusés à tort d'être illicites, et sur le nombre total de décisions imposant des sanctions, y compris une description du type de sanction imposée;

39. se déclare inquiet de la fragmentation des organes de surveillance et de supervision, ainsi que de leur manque avéré en ressources humaines et financières; suggère une coopération accrue entre les États membres en matière de surveillance réglementaire des services numériques;

40. considère que pour garantir une bonne application de la législation sur les services numériques, il convient d'harmoniser au sein du marché unique numérique la surveillance du respect des procédures, des garanties procédurales et des obligations de transparence qui figurent dans ladite législation; souhaite à cet égard que l'application soit suivie de manière solide et rigoureuse par une structure de surveillance de l'Union indépendante, qui puisse imposer des amendes en s'appuyant sur l'évaluation d'un ensemble clairement défini de facteurs, tels que la proportionnalité, les mesures techniques et organisationnelles et la négligence; est d'avis que les amendes devraient pouvoir s'élever à un pourcentage donné du chiffre d'affaires annuel global de l'entreprise;

41. souligne qu'il faut mener les audits des politiques et algorithmes internes des fournisseurs de services numériques dans le respect du droit de l'Union, en particulier des droits fondamentaux des utilisateurs des services, en tenant compte de l'importance de la non-discrimination et de la liberté d'expression et d'information dans une société ouverte et démocratique, et sans publier de données sensibles sur le plan commercial; juge urgent d'évaluer, à la suite d'une plainte ou à l'initiative des organes de surveillance, si les fournisseurs de services numériques amplifient les contenus et de quelle manière, par exemple au moyen de moteurs de recommandation et de fonctions d'optimisation telles que la saisie semi-automatique et les tendances;

42. considère que les rapports de transparence rédigés par les plateformes et les autorités nationales compétentes devraient être rendus accessibles au public et analysés pour repérer des tendances structurelles dans le repérage, le blocage et la suppression de contenus au niveau de l'Union;

43. souligne l'importance de donner aux utilisateurs les moyens de faire respecter eux-mêmes leurs droits fondamentaux en ligne, notamment en facilitant l'accès, pour les particuliers comme les entreprises, à des procédures de plainte impartiales, transparentes, efficaces et gratuites, à des mécanismes de signalement de contenus illicites et de comportements illégaux, ainsi qu'à des recours en justice, et en prévoyant des mesures pédagogiques et des campagnes de sensibilisation aux questions relatives à la protection des données et à la sécurité des enfants en ligne;

44. est d'avis que les expériences passées ont montré que l'on pouvait efficacement permettre à des modèles d'entreprise innovants de prospérer et renforcer le marché unique numérique en supprimant les obstacles à la libre circulation des contenus numériques et en empêchant l'introduction de nouveaux obstacles injustifiés au niveau national; estime que poursuivre cette approche permettra de réduire la fragmentation du marché intérieur; considère en outre que la législation sur les services numériques peut ouvrir des possibilités pour développer les connaissances et les compétences des citoyens dans le domaine numérique et garantir un haut niveau de protection des consommateurs, y compris en préservant la sécurité en ligne;

45. souligne le caractère indispensable d'accords sur les normes de sécurité essentielles dans le cyberespace, de sorte que les services numériques puissent offrir tous leurs avantages aux citoyens; note par conséquent qu'il est urgent que les États membres prennent des mesures coordonnées pour assurer une cyberhygiène de base et pour prévenir les dangers évitables dans le cyberespace, notamment par des mesures législatives;

46. charge son Président de transmettre la présente résolution au Conseil et à la Commission.