



COMMISSION EUROPÉENNE

Bruxelles, 30.4.2018
C(2018) 2440 final

Monsieur le Président,

La Commission tient à remercier l'Assemblée nationale pour son avis sur le marché unique du numérique.

La révolution numérique en cours a le pouvoir de transformer nos sociétés et nos économies, et d'ainsi entraîner des bénéfices à long terme pour la croissance économique et la qualité de nos vies. La stratégie pour le marché unique numérique va au-delà des aspects économiques et a pour but d'assurer que la société européenne affronte la transformation numérique avec confiance et en bénéficie. La stratégie repose sur trois piliers:

- améliorer l'accès aux biens et services numériques,*
- créer un environnement propice au développement des réseaux et services numériques.*
- maximiser le potentiel de croissance de l'économie numérique européenne.*

La stratégie pour le marché unique numérique trace le chemin que l'Union européenne et tous les Etats membres doivent emprunter pour construire un environnement numérique qui assure la confidentialité, la protection des données personnelles et des droits des consommateurs, qui permet aux entreprises d'innover et de concourir, et qui renforce le tissu qui tient ensemble nos sociétés grâce à une cybersécurité renforcée.

La Commission se réjouit du soutien de l'Assemblée nationale aux efforts de l'Union Européenne visant à construire un vrai marché unique numérique européen.

Le dernier rapport sur l'état d'avancement de l'Europe numérique souligne le progrès important de la France en ce qui concerne le numérique, en particulier dans les domaines de l'usage des services de l'administration en ligne et du capital humain - la France étant au premier rang de la formation universitaire en sciences, technologie, ingénierie et mathématiques. Néanmoins, le niveau de connectivité de la France ainsi que le niveau d'intégration des technologies digitales parmi les entreprises françaises étant inférieurs à la moyenne européenne, la France bénéficierait d'une action plus soutenue sur ce front.

*M. François DE RUGY
Président de l'Assemblée nationale
Palais Bourbon
126, Rue de l'Université,
F - 75355 PARIS*

Deux ans et demi après le lancement de la stratégie pour un marché unique numérique, la Commission a proposé quarante-six initiatives. Vingt-sept parmi elles sont des initiatives législatives qui ont été proposées au Parlement européen et au Conseil.

En 2017, des parties clés de la stratégie pour un marché numérique ont été adoptées, notamment la fin des frais d'itinérance, la coordination du spectre, la portabilité du contenu et la mise en œuvre du Traité de Marrakech. Grâce à l'initiative WiFi4EU, les citoyens bénéficieront bientôt d'une connectivité à l'Internet dans les espaces publics. Les ventes en ligne seront facilitées par des règles de taxe sur la valeur ajoutée simplifiées pour les start-ups et les petites et moyennes entreprises, ainsi que par la fin des blocages géographiques injustifiés.

En septembre 2017 la Commission a également approuvé des propositions législatives sur la cybersécurité et la libre circulation des données non personnelles.

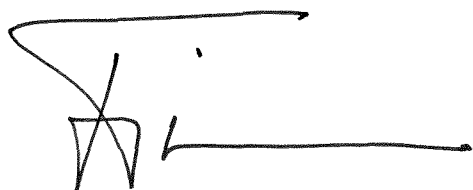
Ensemble nous devons maintenir cet élan et rapidement conclure et mettre en œuvre les propositions restantes afin d'atteindre les objectifs fixés dans la déclaration commune sur les priorités législatives de l'Union pour 2018-2019¹ et l'appel du Conseil européen pour une réalisation complète du marché unique numérique d'ici fin 2018.

Les mesures mentionnées représentent des étapes importantes pour atteindre ce but, mais il nous reste encore beaucoup de chemin à parcourir. Le numérique fait partie d'un programme positif, qui est susceptible de produire des bénéfices rapides aux citoyens européens. L'investissement est un besoin vital et, comme l'Assemblée nationale le souligne dans son avis, la numérisation de l'économie et de la société sont des projets à grande échelle qui nécessitent une action au niveau européen pour réussir. Aucun État membre n'est capable de gérer ces défis tout seul; par conséquent, dans le prochain cadre financier pluriannuel, nous veillerons à ce que des fonds adéquats soient alloués au numérique.

En réponse aux observations plus techniques figurant dans l'avis, la Commission vous invite à consulter l'annexe jointe à cette lettre.

En espérant que ces précisions répondront aux questions soulevées par l'Assemblée nationale, nous nous réjouissons, par avance, de la poursuite de notre dialogue politique.

Veillez agréer, Monsieur le Président, l'expression de notre très haute considération.



*Frans Timmermans
Premier vice-président*



*Mariya Gabriel
Membre de la Commission*

¹ https://ec.europa.eu/commission/publications/joint-declaration-eus-legislative-priorities-2018_fr

Annexe

La Commission a examiné avec soin chacune des questions soulevées par L'Assemblée nationale dans son avis et a l'honneur d'apporter les précisions suivantes.

Point 2, 3 et 5: La Commission remercie l'Assemblée nationale pour le soutien apporté à la proposition de règlement «vie privée et communications électroniques» {COM(2017) 10 final}. La proposition de la Commission prévoit l'extension du champ d'application des règles sur la vie privée aux entreprises fournisseurs de services dites "over-the-top" (OTT). Ceci vise à établir une situation équitable où tous les acteurs fournissant des services de communications électroniques équivalents par leurs fonctions seront sur un même pied d'égalité.

La proposition de la Commission prévoit l'interdiction de stocker ou de collecter des données personnelles sur des terminaux sauf dans les situations bien définies dans l'article 8 de la proposition. Dans son article 9, la proposition détaille la notion de consentement de l'utilisateur final et précise que la définition et les conditions du consentement figurant à l'article 4, paragraphe 11, et à l'article 7 du règlement général sur la protection des données² s'appliquent.

L'article 9 de la proposition prévoit que si cela est techniquement possible et réalisable, le consentement peut être exprimé à l'aide des paramètres techniques appropriés d'une application logicielle permettant d'accéder à l'Internet. La proposition impose aux fournisseurs de logiciels permettant d'accéder à l'Internet l'obligation de faire en sorte qu'au moment de l'installation, les utilisateurs finaux soient informés de la possibilité de choisir leurs paramètres de confidentialité parmi les diverses options proposées et soient invités à opérer un choix. Les navigateurs Web sont encouragés à proposer aux utilisateurs des méthodes simples de changer les paramètres sur la vie privée à tout moment durant l'usage et à leur permettre de faire des exceptions pour certains sites web, de les placer sur des «whitelists» ou de préciser pour quels sites web des cookies (tiers) sont toujours ou jamais permis.

Point 6: Le règlement général sur la protection des données fournit un ensemble unique de règles qui s'appliquent directement dans tous les États membres. Les dispositions du règlement ont un effet direct sur les citoyens, entreprises, administrations publiques et toute autre organisation qui traite des données à caractère personnel.

Néanmoins, en accord avec le règlement, les États membres sont obligés d'adapter leur législation en abrogeant et modifiant les lois existantes ainsi que d'établir une autorité de protection des données, de choisir un organisme accrédité et de mettre en place des règles aptes à réconcilier la liberté d'expression et la protection des données.

De plus, le règlement permet aux États membres de spécifier l'application des règles sur la protection des données dans des domaines spécifiques: le secteur public, l'emploi et la

² Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (Texte présentant de l'intérêt pour l'EEE) ; OJ L 119, 4.5.2016, p. 1–88.

sécurité sociale, la médecine préventive et occupationnelle, la santé publique, l'usage des données à des fins d'archivage dans l'intérêt public ou de recherches historiques ou statistiques, le numéro d'identification national, l'accès public aux documents officiels et l'obligation de confidentialité.

En outre, pour les données génétiques et biométriques ainsi que les données concernant la santé, le règlement habilite les États membres de maintenir ou introduire des conditions supplémentaires ou des limitations.

Cependant, les actions des États membres sont encadrées par deux éléments:

- 1. Article 8 de la Charte des droits fondamentaux de l'Union européenne³: chaque droit national de spécification doit garantir les exigences de l'article 8 de la Charte (et de la réglementation basée sur l'article 8 de la Charte), et*
- 2. Article 16(2) du Traité sur le fonctionnement de l'Union européenne, selon lequel aucune législation nationale ne peut empiéter sur la libre circulation des données au sein de l'Union européenne.*

Le règlement présente une opportunité importante pour simplifier l'environnement légal, d'avoir moins de règles nationales et d'ainsi entraîner plus de clarté pour les opérateurs.

Lorsque les États membres adaptent leur législation nationale, il leur est demandé de tenir compte du fait que les mesures nationales qui ont pour résultat de faire obstacle aux effets directs du règlement et de compromettre l'application simultanée et uniforme du règlement dans l'ensemble de l'Union européenne sont contraires aux traités⁴.

Point 7: La proposition de règlement «vie privée et communications électroniques» précise dans son article 11 à quelles fins et conditions les États membres peuvent restreindre l'application des dispositions du règlement. La proposition prévoit la possibilité, par la voie de mesures législatives, de limiter la portée des obligations et des droits prévus aux articles 5 à 8 lorsqu'une telle limitation respecte l'essence des libertés et droits fondamentaux et qu'elle constitue une mesure nécessaire, appropriée et proportionnée dans une société démocratique pour préserver un ou plusieurs des intérêts publics visés à l'article 23, paragraphe 1, points a) à e), du règlement (UE) 2016/679, ou une fonction de contrôle, d'inspection ou de réglementation participant à l'exercice de l'autorité publique relativement à ces intérêts.

Point 8: La Commission est convaincue que cette question est entièrement traitée par l'ensemble unique de règles fourni par le règlement général sur la protection des données. Tout traitement de données personnelles doit avoir une base juridique valable sous l'article 6 de ce règlement.

³ OJ C 326, 26.10.2012, p. 391–407.

⁴ Voir la Communication de la Commission au Parlement européen et au Conseil, "Une meilleure protection et de nouvelles perspectives - Orientations de la Commission relatives à l'application directe du règlement général sur la protection des données à partir du 25 mai 2018" / COM(2018) 43 final, 24.01.2018.

Le consentement représente une des options mentionnées sous l'article 6 du règlement. Cependant, cela n'est pas toujours la base la plus appropriée pour le traitement des données. Pour cela, les autres bases juridiques peuvent également être considérées par l'organisation traitant les données.

Lorsqu'un consentement est demandé aux individus pour le traitement de leurs données, le règlement général sur la protection des données renforce les exigences pour obtenir un tel consentement. Article 4(11) du règlement général constate que le consentement se définit comme "toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement". De plus, l'article 7 du règlement général établit des conditions spécifiques pour obtenir ce consentement.

Points 9 à 11: La Commission tient à remercier l'Assemblée nationale pour sa Résolution concernant la proposition de la Commission pour un règlement concernant un cadre applicable à la libre circulation des données à caractère non-personnel dans l'Union européenne {COM (2017) 495 final}.

En ce qui concerne la sécurité des données non personnelles, la cybersécurité fait déjà l'objet de réglementations dans le cadre de la directive (EU) 2016/1148 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union ainsi que dans la nouvelle proposition de règlement du Parlement européen et du Conseil relatif à l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) et à la certification des technologies de l'information et des communications en matière de cybersécurité {COM(2017) 477 final}.

Concernant le cadre européen de certification que cette dernière proposition vise à établir en matière de cybersécurité des produits et services, les services de la Commission ont déjà entamé des discussions avec l'industrie relatives à un système de certification européenne pour les services de technologies en nuage. Ces discussions se poursuivront dans les mois à venir avec les parties prenantes.

La Commission se félicite du soutien de l'Assemblée nationale sur l'aspect de la portabilité des données non personnelles. Lors de l'étape d'analyse et de préparation de la proposition sur la libre circulation des données non personnelles, la Commission a conclu que la question de circulation de données entre différents systèmes et services informatiques (notamment en cas de changement d'hébergeur de données) devrait être traitée en premier lieu par des mesures stimulant l'auto-régulation, ceci afin d'intervenir de manière proportionnée et de tenir compte du peu de données quantitatives disponibles sur les aspects économiques pour les fournisseurs et pour les utilisateurs.

De plus, l'option du code de conduite proposée dans la proposition sur la libre circulation des données non personnelles, permettrait de bénéficier directement de l'expertise technologique des parties prenantes, dans un domaine posant des nombreuses questions à caractère technique.

Points 12 à 14: En ce qui concerne les questions soulevées sur le cadre de certification en matière de cybersécurité, la Commission a pleinement pris en compte les expériences nationales et européennes et vise à tirer le meilleur parti de celles-ci dans le cadre européen. La décision de confier à l'agence de cybersécurité européenne un rôle important dans l'exercice de certification se fonde sur une analyse approfondie des options disponibles. Cette analyse a clairement mis en évidence la nécessité de disposer d'un organe indépendant de l'Union européenne, actif dans le domaine, afin de soutenir la création et le maintien du cadre et que l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) est le seul organe de l'Union présentant de telles caractéristiques.

En outre, alors que l'agence de cybersécurité européenne jouera un rôle dans l'élaboration des régimes de certification, le fonctionnement de ces systèmes, y compris l'analyse de produits dans des laboratoires, la délivrance de certificats, le suivi et l'exécution resteront de la compétence des États membres et seront réalisés au niveau national.

En ce qui concerne la gouvernance de ce cadre, les États membres sont appelés à jouer un rôle fondamental par l'intermédiaire du Groupe européen de cybersécurité de certification établi par la proposition en assistant la Commission et l'agence de cybersécurité européenne dans l'élaboration et le réexamen des régimes de certification, et via la procédure d'examen sur les actes d'exécution qui définiront chaque régime.

Point 15: En ce qui concerne la version révisée du mandat de l'agence de cybersécurité européenne, la proposition de la Commission {COM(2017) 477 final} autorise l'agence à appuyer les travaux des États membres et des institutions de l'Union en vue d'atteindre la résilience collective de l'Union. Plus spécifiquement, les tâches qui ont été confiées à l'agence en ce qui concerne la coopération opérationnelle sont fondées sur les dispositions de la directive (UE) 2016/1148, qui confie à l'Agence européenne chargée de la sécurité des réseaux et de l'information le secrétariat du réseau des équipes de la réaction aux incidents touchant la sécurité informatique; sur les dispositions de l'actuel règlement⁵, qui prévoit déjà la possibilité pour les États membres et les institutions de l'Union de demander de l'aide en cas de violation de la sécurité ayant un impact significatif; et sur les nouvelles initiatives stratégiques au niveau de l'Union (en particulier, le «schéma directeur» défini dans la recommandation sur la coordination de la réaction aux incidents de cybersécurité à grande échelle et des crises). Ces missions ne doivent pas remplacer ou faire double emploi avec les fonctions et les responsabilités des États membres. Au contraire, elles sont mises en œuvre afin d'aider les États membres à améliorer leur capacité à prévenir, détecter et réagir à des incidents et à contribuer à la coopération opérationnelle au niveau de l'Union, en particulier en ce qui concerne les questions transfrontalières.

⁵ Règlement (UE) 526/2013 du Parlement européen et du Conseil du 21 mai 2013 concernant l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) et abrogeant le règlement (CE) 460/2004; OJ L 165, 18.6.2013, p. 41–58.

Point 17: Les règles d'impôts sur les sociétés ont été conçues dans l'ère pré-Internet et sont confondues par les entreprises digitales, globalisées et mobiles d'aujourd'hui. Elles reposent dans une grande partie sur le concept de la présence physique et sont soutenues par le simple principe que les profits devraient être imposés à l'endroit de la création de la valeur. La numérisation a profondément ébranlé ce principe. Dans un monde numérisé, il peut être difficile de déterminer la valeur créée, comment elle a été créée et où elle devrait être imposée.

Dans l'Union européenne, il est devenu assez commun pour une entreprise d'avoir une présence digitale significative dans un État membre et d'y générer des profits importants, alors qu'elle bénéficie ailleurs d'un niveau d'impôts proche de zéro.

Point 18: La Commission est fermement convaincue que la solution ultime pour ces défis doit être globale. Les Ministres des Finances du G20 ont chargé l'Organisation de Coopération et de Développement Économiques de la production avant avril 2018 d'un rapport intérim sur les implications de l'imposition du numérique. La Commission travaille étroitement avec l'Organisation de Coopération et de Développement Économiques pour soutenir le développement d'une solution internationale.

Suite à la requête en décembre 2017 du Conseil pour les Affaires économiques et financières (ECOFIN), la Commission a présenté une initiative sur les règles d'imposition des sociétés ayant une présence numérique significative⁶.

De plus, la Commission considère des mesures ciblées plus immédiates pour répondre aux lacunes plus critiques dans nos systèmes d'impôts sur les sociétés en ce qui concerne l'imposition du numérique, et la prévention des charges inutiles pour les entreprises à cause d'un patchwork des réglementations nationales dans le marché unique.

Point 19: La Commission se réjouit du soutien apporté par l'Assemblée nationale à la proposition de directive sur le droit d'auteur dans le Marché unique numérique et prend note de l'appel à une implication renforcée des plateformes, laquelle est en parfaite cohérence avec les initiatives de la Commission.

La question du partage de la valeur créée par les nouveaux usages en ligne est un aspect clé de la proposition de directive. Il s'agit d'établir un marché qui fonctionne de manière équitable, notamment compte tenu du rôle joué par certaines plateformes en ligne dans l'accès aux contenus par le public. Dans ce cadre, la Commission a proposé un nouveau droit voisin pour les éditeurs de presse avec l'objectif de renforcer un secteur essentiel à la démocratie.

Ce nouveau droit renforcera la position des éditeurs lors de négociations avec d'autres acteurs du marché quant à l'usage de leurs contenus en ligne et il permettra d'agir de façon plus efficace contre les usages illégaux de leurs contenus.

⁶ Proposition de Directive du Conseil établissant les règles d'imposition des sociétés ayant une présence numérique significative; COM(2018) 147 final.

La Commission a proposé par ailleurs une nouvelle obligation pour les services de partage de contenus qui ont un impact important sur le marché de la distribution de contenus en ligne de prendre des mesures afin de renforcer le contrôle des ayants droit sur la présence et l'utilisation de leurs contenus sur ces sites. Cette mesure permettra aux ayants droit d'être dans une meilleure position pour négocier les conditions d'utilisation de leurs contenus en ligne. Enfin la Commission a proposé de renforcer les obligations des cessionnaires de droits dans le but de donner plus de transparence pour les auteurs et artistes interprètes sur l'exploitation de leurs créations et sur les revenus générés, et renforcer ainsi leur position de négociation.

En parallèle, la Commission a adopté une série de mesures destinées à lutter de façon horizontale contre les contenus illicites. En particulier, dans sa Communication du 29 novembre 2017 qui concerne la directive de 2004⁷ sur le respect des droits de propriété intellectuelle, elle a, afin de renforcer l'efficacité de la directive, adopté des orientations qui apportent des clarifications sur les dispositions de la directive ayant donné lieu à des interprétations divergentes dans les États membres. Elle est par ailleurs engagée dans une promotion d'accords volontaires avec les acteurs de différents secteurs (ex: places de marché en ligne, acteurs du secteur de la publicité) en vue de limiter la contrefaçon en ligne ou de limiter son attractivité économique (approche dite «Follow the money» ou «Frapper au portefeuille»).

Point 20: La Commission a entamé un dialogue avec les plateformes en ligne pour obtenir leur engagement dans l'application des mesures prévues dans la communication «Lutter contre le contenu illicite en ligne. Pour une responsabilité accrue des plateformes en ligne» du 28 septembre 2017.

La Commission a aussi adopté une Recommandation le 1 mars 2018 pour avancer dans la même direction encore plus rapidement et avec plus de force, particulièrement dans le domaine de la lutte contre le contenu terroriste en ligne⁸.

Point 21: La proposition pour la révision de la directive de services de médias audiovisuels⁹ adoptée par la Commission en mai 2016 prévoit une extension limitée de son champ d'application aux plateformes de partage de vidéos.

Les nouvelles règles prévues dans la proposition de directive feront en sorte que les plateformes de partage de vidéos mettent en place des mesures appropriées (contrôle parental et systèmes de vérification de l'âge) pour protéger les mineurs des contenus qui leur sont préjudiciables. L'opportunité de telles mesures sera évaluée par les autorités réglementaires nationales. La directive fournira donc aux autorités de régulation

⁷ Communication de la Commission au Parlement européen, au Conseil et au Comité économique et social européen. Un système équilibré de contrôle du respect de la propriété intellectuelle pour relever les défis sociétaux d'aujourd'hui ; COM(2017) 707 final.

⁸ Recommandation de la Commission du 1.3.2018 sur les mesures destinées à lutter, de manière efficace, contre les contenus illicites en ligne ; C(2018) 1177 final.

⁹ Proposition de Directive du Parlement européen et du Conseil 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, compte tenu de l'évolution des réalités du marché; COM(2016) 287 final.

nationales un appui législatif en cas de non-respect par les plateformes, y compris l'imposition de sanctions conformément à la législation nationale.

Point 22: Compte tenu du fait qu'un utilisateur d'Internet sur trois est un enfant, assurer un environnement en ligne sûr pour les enfants est une des priorités de la Commission. Un environnement numérique sûr et stimulant pour les enfants est une responsabilité commune et nécessite, de fait, une approche multipartite.

De son côté, à travers la Stratégie européenne pour un Internet mieux adapté aux enfants¹⁰, la Commission continue à assurer la coordination, le soutien financier et la contribution à un cadre réglementaire adaptés aux nouveaux défis. Elle travaille sur l'ensemble de la gamme des actions possibles avec le Parlement européen, les États membres, l'industrie, les universités, les organisations non gouvernementales et les jeunes eux-mêmes pour offrir un environnement numérique plus sûr, mais aussi un meilleur environnement numérique au service des citoyens européens.

Tout récemment, à l'occasion du 15ème «Safer Internet Day», la Commissaire pour l'économie et la société numériques, Mariya Gabriel, a lancé au Parlement européen à Strasbourg la campagne #SaferInternet4EU à l'échelle de l'Union européenne, qui se déroulera tout au long de l'année 2018. Les initiatives encourageront la «cyber-hygiène», l'éducation aux médias, la pensée critique et les compétences numériques. Les principaux acteurs du paysage numérique et médiatique seront impliqués, y compris les centres «Safer Internet en Europe».

¹⁰ Communication de la Commission au Parlement européen, au Conseil, au Comité Économique et Social Européen et au Comité des Régions Stratégie européenne pour un Internet mieux adapté aux enfants ; COM(2012) 196 final.