N° 479

ASSEMBLÉE NATIONALE

CONSTITUTION DU 4 OCTOBRE 1958

QUINZIÈME LÉGISLATURE

Enregistré à la Présidence de l'Assemblée nationale le 6 décembre 2017.

RAPPORT D'INFORMATION

DÉPOSÉ

PAR LA COMMISSION DES AFFAIRES EUROPÉENNES [1]

sur le **marché unique** du **numérique**

ET PRÉSENTÉ

PAR M. ÉRIC BOTHOREL et Mme CONSTANCE LE GRIP,
Députés

(1) La composition de la commission figure au verso de la présente page.

La Commission des affaires européennes est composée de : Mme Sabine THILLAYE, *présidente* ; MM. Pieyre-Alexandre ANGLADE, Jean-Louis BOURLANGES, Bernard DEFLESSELLES, Mme Liliana TANGUY, *vice-présidents* ; Mme Sophie AUCONIE, M. André CHASSAIGNE, Mmes Marietta KARAMANLI, Danièle OBONO, *secrétaires ;* MM. Damien ABAD, Patrice ANATO, Mmes Aude BONO-VANDORME, MM. Éric BOTHOREL, Vincent BRU, Mmes Fannette CHARVIER, Yolaine de COURSON, Typhanie DEGOIS, Marguerite DEPREZ-AUDEBERT, M. Benjamin DIRX, Mmes Coralie DUBOST, Françoise DUMAS, MM. Pierre-Henri DUMONT, Alexandre FRESCHI, Bruno FUCHS, Mmes Valérie GOMEZ-BASSAC, Carole GRANDJEAN, Christine HENNION, MM. Michel HERBILLON, Alexandre HOLROYD, Christophe JERRETIE, Jérôme LAMBERT, Mmes Constance Le GRIP, Nicole Le PEIH, MM. Jean-Claude LECLABART, Ludovic MENDES, Thierry MICHELS, Christophe NAEGELEN, Mme Valérie PETIT, MM. Damien PICHEREAU, Jean-Pierre PONT, Joaquim PUEYO, Didier QUENTIN, Mme Maina SAGE, MM. Raphaël SCHELLENBERGER, Benoit SIMIAN, Éric STRAUMANN, Mmes Michèle TABAROT, Alice THOUROT.

SOMMAIRE

___

Pages

INTRODUCTION

Mesdames, Messieurs,

La Commission européenne progresse à l'heure actuelle – à grands pas – vers la conclusion de sa stratégie pour un marché unique du numérique. Il s'agissait là d'une des grandes priorités politiques de la Commission de Jean-Claude Juncker et l'activité de la présidence estonienne à cet égard témoigne de l'importance du sujet.

Le marché unique du numérique comprend par définition un vaste éventail de secteurs, tous touchés par la révolution digitale. L'ambition première qui préside à cette politique est donc de faire advenir un marché intérieur dans lequel la grande majorité des barrières nationales injustifiées auraient disparu, en vue de faciliter les échanges et notamment la circulation des données. Cette ambition initiale, destinée à favoriser la croissance d'entreprises numériques qui souffrent encore trop souvent, en France et en Europe, d'une petite taille par rapport à leurs concurrents mondiaux, s'est doublée d'une seconde dimension : la volonté de réguler le secteur numérique.

Les bouleversements technologiques récents nécessitent en effet une adaptation de la législation de l'Union sur, là encore, un vaste champ d'actions, de la valorisation des œuvres culturelles au respect d'une juste contribution aux budgets publics. Les questions de sécurité et de protection de la vie privée justifient également l'intervention publique.

C'est dans cette perspective que vos rapporteurs ont souhaité aborder cet ensemble très hétérogène sous l'angle des propositions récentes en matière de législation européenne, et plus précisément par le biais de quatre axes.

En premier lieu, la proposition de règlement dite « *ePrivacy* », qui vise à adapter les principes de protection des données personnelles issus du Règlement général de protection des données (RGPD) au domaine des télécommunications, tire sa légitimité de l'obsolescence des textes précédents. L'irruption de nouveaux acteurs dits « over the top » justifie en effet une adaptation de la législation à la nouvelle donne technologique. Ces nouveaux acteurs des télécommunications, dits aussi « services par contournement », permettent d'échanger des données sans passer par les biais habituels que sont les compagnies de câble ou de satellite. Des exemples de telles compagnies sont connus : WhatsApp, Facebook Messenger entrent, parmi d'autres, dans cette catégorie.

Il n'en demeure pas moins que, pour vos rapporteurs, la notion de consentement parfaitement pertinente dans le cadre du RGPD doit s'appliquer aux traceurs, dits « cookies », sans pour autant compromettre le développement de

services numériques à valeur ajoutée dont le modèle économique repose sur l'exploitation des données à des fins publicitaires.

Le projet de règlement visant à favoriser la libre circulation des données non-personnelles au sein de l'Union européenne recueille également la faveur de vos rapporteurs, qui souhaitent rappeler qu'au sein du marché unique du numérique, il faut avant tout favoriser la dimension de marché. Dès lors, les restrictions nationales injustifiées à la circulation de ces données, la localisation forcée des données en fonction de considérations stratégiques parfois faussées sont autant d'obstacles à la formation d'ensembles de données susceptibles d'être ensuite traitées par des entreprises européennes et, partant, contribuer à leur croissance.

Il demeure que la localisation forcée des données peut se justifier dans certains cas. Ainsi, il peut également apparaître légitime que les États puissent conserver ce qui relève des archives publiques et des trésors nationaux au sein de leur territoire.

Le « paquet » cybersécurité, qui s'articule principalement autour de la proposition de règlement visant à étendre le mandat de l'ENISA, l'Agence européenne de cybersécurité, traduit là encore une approche communautaire de questions touchant à des dimensions régaliennes. C'est pourquoi le renforcement de l'action de l'ENISA ne peut se traduire, pour vos rapporteurs, par l'affaiblissement des modalités d'action des agences nationales, sans quoi le niveau de cybersécurité européen pourrait en pâtir. C'est au contraire sur la collaboration entre les agences nationales et l'agence européenne, ainsi que sur l'adoption d'un système de certification ambitieux mais proportionné aux nécessités de certification propres à chacun des services numériques échangé au sein du marché intérieur que doit porter l'effort de législation européenne.

Vos rapporteurs ont également souhaité saluer et accompagner l'initiative française en faveur d'une « taxe d'égalisation » pour les entreprises numériques. Il ne s'agit, certes, que d'un premier pas vers la mise en place d'un système fiscal efficace et juste à l'échelle de l'Union. Il s'agirait néanmoins d'un outil nécessaire, dans l'attente des conclusions des travaux de l'OCDE à ce sujet, au printemps 2018 et de la mise en place d'une Assiette Commune Consolidée pour l'Impôt des Sociétés (ACCIS).

Enfin, si ce point n'a pas fait l'objet d'une réflexion approfondie dans le cadre de cette mission, vos rapporteurs ont relevé avec intérêt le développement des réflexions actuelles sur l'économie des plateformes. Celles-ci structurent déjà en grande partie les pratiques quotidiennes de millions d'Européens sur Internet. Ce statut emporte des responsabilités, notamment à l'égard de la juste valorisation des œuvres culturelles par le respect des principes du droit d'auteur et de la lutte contre la propagation de discours haineux ou faisant l'apologie du terrorisme.

PREMIÈRE PARTIE : LA PROTECTION DES DONNÉES PERSONNELLES DANS LE SECTEUR DES TÉLÉCOMMUNICATIONS

I. L'AMBITION DE LA COMMISSION EUROPÉENNE : ASSURER UN NIVEAU DE PROTECTION ÉQUIVALENT À CELUI DU RÈGLEMENT GÉNÉRAL DE PROTECTION DES DONNÉES (RGPD) DANS LE DOMAINE DES TÉLÉCOMMUNICATIONS

Ainsi que l'a expliqué M. Grégoire Tirot, directeur de cabinet du Secrétaire d'État au numérique, l'ensemble des initiatives législatives en faveur de l'établissement d'un marché unique du numérique est très foisonnant. Il se compose dans son ensemble de 35 initiatives, ce qui, compte tenu des efforts actuels de la Commission européenne pour mieux maîtriser l'activité législative européenne, est remarquable.

De ce patchwork ressort au départ une volonté de la Commission européenne de faire tomber tous les obstacles nationaux qui entraveraient de manière injustifiée l'émergence de ce marché. Désormais, la stratégie pour un marché unique du numérique se concentre également sur la nécessaire régulation de ce secteur, notamment en termes de traitement des données. La proposition de règlement *ePrivacy* participe de cette volonté, à la suite du Règlement général de protection des données.

A. LA PROTECTION DES DONNÉES INSTITUÉE PAR LE RGPD REPOSE SUR LE CONSENTEMENT ET LE PASSAGE À UNE LOGIQUE DE RESPONSABILISATION DES ACTEURS

1. Les principes fondateurs du RGPD

Le RGPD a traduit, après de longues années de négociation, la capacité de la Commission européenne de créer un cadre aussi unifié que possible de protection des données. Cette harmonisation est particulièrement bienvenue au moment où les données s'échangent de manière exponentielle, sans que pour autant les utilisateurs aient une conscience nette de ce que peut impliquer le partage de ces données.

Le texte a déjà fait l'objet de nombreuses études et rapports, dont celui de Mme Anne-Yvonne Le Dain et M. Philippe Gosselin pour la Commission des Lois [(1)], afin d'en évaluer l'impact sur la législation française. L'ampleur du texte tient notamment à sa conception large de concepts aussi fondamentaux que le consentement ainsi que son champ d'application. La réforme de l'ancienne

(1) Rapport d'information déposé le 22 février 2017 sur les incidences des nouvelles normes européennes en matière de protection des données personnelles sur la législation française.

directive 95/46/CE du 24 octobre 1995 [(1)] s'était appuyée sur une communication de la Commission européenne dès 2012 [(2)].

L'article 4 définit ainsi les données à caractère personnel comme « toute information se rapportant à une personne physique identifiée ou identifiable […] ; est réputée être une « personne physique identifiable » une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale ». Cette définition est reprise par la proposition de règlement *ePrivacy*, mais élargie aux métadonnées dans la mesure où le traitement de ces dernières peut conduire à identifier une personne et la classer selon des critères dégagés par le RGPD. Ce règlement adapte aux technologies actuelles la réglementation relative aux techniques d'identification, afin d'en renforcer l'efficacité technique.

C'est également du RGPD qu'est issue la définition du consentement que l'on peut retrouver dans la proposition de règlement *ePrivacy*. Alors que la directive de 1995 ne faisait qu'exiger le caractère indubitable du consentement donné, la complexité technique liée notamment au consentement forcé en cas de répétition des demandes ou encore les faibles connaissances que détiennent les utilisateurs quant aux conséquences de leur consentement ont abouti à faire évoluer la définition. Celle-ci se structure désormais autour de la notion de consentement explicite, telle que la développe l'article 4 du RGPD : « 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 ». Dès lors, le consentement n'est pas présumé libre lorsque des conditions préalables sont exigées, telles que l'accès à un service numérique, en échange de l'acceptation.

Outre ces définitions applicables également au règlement *ePrivacy* en cours de négociation, le RGPD a contribué à renverser la logique de responsabilité des acteurs du numérique. Il consacre en effet un changement de paradigme impliquant la responsabilisation des acteurs traitant des données. Ces derniers, déchargés de nombreuses obligations déclaratives *a priori* auprès des autorités nationales en charge du respect de la confidentialité des données personnelles, devront notamment tenir un registre des activités de traitement et, surtout, désigner un délégué à la protection des données, chargé entre autres de vérifier la bonne application du règlement et de notifier aux autorités compétentes toute brèche dans la protection des données personnelles.

---

(1) Directive 95/46/CE du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation des données.

(2) Communication de la Commission européenne, « Protection de la vie privée dans un monde en réseau », 25 mai 2012.

Enfin, ainsi que l'a présenté Jean Lessi, l'actuel secrétaire général de la CNIL, le RGPD a vocation à s'appliquer également aux entreprises américaines et chinoises lorsqu'elles ciblent des citoyens européens. En cela, il s'agit de l'affirmation d'une souveraineté juridique européenne bienvenue. Pour la CNIL, le RGPD implique également un changement de méthode. Les régulateurs nationaux vont en effet fonctionner en réseau, notamment au sein du comité européen institutionnalisant les pratiques de l'actuel G29, forum informel de coopération entre les autorités de régulation du numérique. Ce comité aura la charge de définir la jurisprudence commune aux États membres, dans l'épure du RGPD, ce qui amènera à ce que l'ensemble du secteur soit régulé de manière harmonisée à l'échelle européenne.

Il consacre enfin l'alourdissement considérable des amendes que les autorités de régulation peuvent prononcer à l'encontre d'acteurs privés ne se conformant pas au RGPD. Le règlement donne aux autorités de contrôle la possibilité de prononcer des amendes administratives qui peuvent atteindre, selon la catégorie de l'infraction, 10 ou 20 millions d'euros, ou, dans le cas d'une entreprise, de 2 % jusqu'à 4 % du chiffre d'affaires annuel mondial, le montant le plus élevé étant retenu.

L'originalité du RGPD tient enfin à ce que, si ces principes ont vocation à s'appliquer d'une manière harmonisée et dans tous leurs éléments à l'ensemble des États membres, le Règlement laisse une grande marge de manœuvre aux États membres, de telle sorte que 57 points peuvent encore faire l'objet d'adaptations nationales. Les risques induits de fragmentation réglementaire en matière de gestion des données personnelles s'expliquent entre autres par la complexité du sujet, la sensibilité de nombreuses questions liées notamment à l'accès aux données personnelles à des fins de sécurité publique et à la longueur des négociations, qui ont duré près de quatre ans.

L'adaptation de la législation nationale, et en particulier la réforme de la loi dite « Informatique et libertés » [(1)] sera donc nécessaire avant que le Règlement n'entre en vigueur, soit le 25 mai 2018. Ainsi que l'a présenté M. Jean Lessi, secrétaire général de la CNIL, cette adaptation doit se faire aussi vite que possible, compte tenu du fait que la France fait désormais partie des derniers États membres à ne pas avoir encore fait de choix au sein des marges de manœuvre que laisse le RGPD. Vos rapporteurs estiment que l'adaptation de la loi Informatique et Libertés doit désormais intervenir aussi rapidement que possible, afin de :

- ne pas amoindrir l'effort des acteurs privés français, qui ont déjà mis en place les solutions techniques de conformité au RGPD, sans connaître l'usage que feront les autorités nationales de leurs marges de manœuvre au sein du règlement ;

(1) Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés

- vérifier que l'adaptation nationale ne contribue pas à l'augmentation de la fragmentation européenne en la matière. Ainsi que l'ont expliqué à vos rapporteurs les représentants de la DG JUST, si les États membres demeurent souverains dans les options laissées ouvertes par la Commission européenne, un rapprochement aussi grand que possible entre les législations nationales permettrait d'éviter l'apparition de nouvelles divergences dans le domaine de la protection des données personnelles.

2. L'adaptation des acteurs publics et privés au RGPD

Les apports du RGPD pour la protection des utilisateurs ne sont donc pas contestables, mais l'application de ce règlement au 25 mai 2018 suppose toutefois une réelle adaptation de la part des entreprises privées concernées. Les acteurs privés auditionnés, tels qu'Orange, ont fait part à vos rapporteurs de leurs efforts pour aboutir à une conformité totale aux dispositions du Règlement. Il a toutefois été relevé que cette application entraînait des disparités entre les acteurs économiques du numérique, malgré les nombreux efforts que les représentants de la DG JUST ont mentionnés. Ces derniers ont en effet tenu de nombreuses rencontres avec les parlements nationaux ainsi qu'avec les gouvernements des États membres afin d'expliquer les conséquences précises du Règlement. Les représentants du cabinet du Commissaire et vice-président de la Commission Andrus Ansip, que vos rapporteurs ont rencontré à Bruxelles, ont souligné la valeur de ce travail en ce qu'il devait permettre de limiter la divergence entre les entreprises exerçant leur activité au sein de l'Union européenne dans l'application du RGPD. Le G29, forum de travail en coopération des autorités nationales de régulation, va également dans ce sens, puisqu'il prépare des lignes directrices destinées à uniformiser l'application du règlement. Ces lignes directrices engagent les États membres. Quatre d'entre elles ont déjà été adoptées et d'ici 2018, huit à dix lignes directrices devraient être conclues.

Le RGPD emporte en effet de nombreuses conséquences, y compris pour les collectivités publiques. La désignation d'un référent en charge de la bonne application du règlement, et donc du respect de la confidentialité dans le traitement des données personnelles, constitue un véritable effort de formation et de prévision en matière de ressources humaines. Les représentants de Google ont précisé à vos rapporteurs avoir pu consulter une étude du MEDEF selon laquelle seuls 10 % des entreprises interrogées étaient prêtes à se conformer au RGPD. À ce titre, le secrétaire général de la CNIL a appelé à « tirer la sonnette d'alarme. » Si la plupart des grandes entreprises ont entrepris de se mettre en conformité avec le règlement, il convient de sensibiliser encore les têtes de réseau, s'appuyer sur les professionnels, pour décliner les actions concrètes au sein des TPE/PME. De la même manière, des acteurs publics comme l'Association des Départements de France se sont emparés de cette question en élaborant des chartes de pratiques, mais cette question demeure encore trop confidentielle.

Or, les représentants de Microsoft, par exemple, qui sont, dans le cadre de leurs activités, en contact avec de nombreux acteurs tant publics que privés, ont

alerté vos rapporteurs sur la difficulté que nombre d'entre eux avaient pour être en conformité totale avec le Règlement. De la même manière, M. Schmutz, représentant du CISPE (*Cloud Infrastructure Services Providers in Europe*) a évoqué avec vos rapporteurs le code de bonne conduite qu'OVH avait institué afin de préparer au mieux sa conformité avec le RGPD. Il s'agit là d'un exemple concret de ce qui peut être mis en pratique pour assurer une conformité rapide au RGPD. La CNIL a également la mission d'accompagner les acteurs privés français dans cette transition délicate, et mobilise notamment des *packs* dans différents secteurs tels que l'assurance, le véhicule connecté ou l'automobile pour construire des solutions opérationnelles et applicables aussi rapidement que possible.

Dans l'ensemble, ainsi que M. Loesekrug-Pietri l'a expliqué lors de son audition, les entreprises européennes qui auront fait l'effort de se mettre en conformité rapidement avec le RGPD et donc d'assurer un niveau de protection des données personnelles presque sans équivalent devraient en faire un argument dans la vente de leurs produits. Il convient de faire en sorte que l'avènement d'un marché unique du numérique avec des hauts standards de certification n'entraîne pas seulement des difficultés pour les entreprises européennes, à commencer par les PME, mais que ces dernières puissent se targuer de leur expérience pour exporter des produits haut de gamme. Les représentants de Qwant ont aussi insisté sur la nécessité de faire de la conformité à l'encadrement des données personnelles un argument permettant aux utilisateurs de faire la différence entre différents produits. Ils ont expliqué à vos rapporteurs leur conformité initiale au RGPD et à toutes les directives de la CNIL. Ils se sont ainsi présentés comme « le seul moteur de recherche qui respecte la vie privée », via la *privacy by design*. La pratique de la minimisation de données [(1)] permet donc d'aller plus loin que le cadre prévu par le RGPD. Ce positionnement leur permet de compter aujourd'hui 51 millions de visites uniques.

B. UNE ÉQUIVALENCE POUR LE DOMAINE DES TÉLÉCOMMUNICATIONS : LE RÈGLEMENT « EPRIVACY »

1. La directive 2002/58/CE était devenue largement obsolète

Le texte traitant des questions de la protection des données personnelles dans le cadre des télécommunications était la directive 2002/58/CE du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques).

Il convient de noter que la protection des données personnelles s'appuie sur une longue tradition juridique visant à protéger le secret des correspondances et respecter la vie privée des citoyens. Ces principes sont exprimés tout autant au

(1) Article 5 du Règlement général de protection des données : « Les données à caractère personnel doivent être (…) adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (minimisation des données) »

sein de la Charte des droits fondamentaux, en son article 7, que par l'article 8, paragraphe 1 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales.

Cette directive a établi, en conformité notamment avec la Charte des droits fondamentaux, les principes directeurs de protection de la vie privée et des données personnelles en matière de télécommunication. Le texte visait avant tout à :

- adopter des dispositions législatives, règlementaires et techniques spécifiques afin de protéger les droits et les libertés fondamentaux des personnes physiques et les intérêts légitimes des personnes morales, notamment eu égard à la capacité accrue de stockage et de traitement automatisés de données relatives aux abonnés et aux utilisateurs ;

- assurer la sécurité du réseau public de communication, afin que seules les personnes autorisées puissent avoir accès aux données à caractère personnel à des fins légalement autorisées ;

- obliger les opérateurs à effacer ou rendre anonymes les données relatives au trafic concernant les abonnés et les utilisateurs dès lors qu'elles ne sont plus nécessaires à la transmission d'une communication, sauf les données nécessaires à établir une facture et des limitations constituant des mesures nécessaires, appropriées et proportionnées au sein d'une société démocratiques pour sauvegarder la sécurité nationale ;

- garantir la libre circulation des données, équipements et services de communications électroniques dans l'Union.

Si ces principes conservent toute leur validité, la directive se concentrait avant tout sur les télécommunications par voie analogique et traitait, entre autres, des renvois d'appel automatiques. Or, le contexte technologique relatif aux télécommunications a grandement évolué en quinze ans et l'obsolescence de certains aspects de la directive a été relevée par la Commission lors de son évaluation dite REFIT [(1)]. C'est pourquoi la Commission européenne a intégré dans le champ d'application de la proposition de règlement « les fournisseurs de services de communications électroniques, les fournisseurs d'annuaires accessibles au public et les fournisseurs de logiciels permettant des communications électroniques, y compris la récupération et la présentation d'informations sur Internet, ainsi que les personnes physiques et morales utilisant des services de communications électroniques pour envoyer des communications commerciales de prospection directe ou recueillir des informations qui concernent l'équipement terminal de l'utilisateur final ou qui y sont stockées. »

En particulier, nombreux sont les individus et les entreprises à user de nouveaux acteurs pour transmettre des messages. Il s'agit principalement de services sur internet de messagerie instantanée, appelés « services de

(1) Ex-post REFIT evaluation of the ePrivacy Directive 2002/58/EC, du 10 janvier 2017.

communication par contournement », ou acteurs « *over the top* », ci-après OTT. Des exemples de ces nouveaux acteurs ont été développés par Facebook, à l'instar de Facebook Live, ou se sont développés par eux-mêmes, comme le montre l'exemple de WhatsApp. Il peut s'agir également de services de communications interpersonnelles, fondés ou non sur la numérotation, comme par exemple la voix sur IP, les services de messagerie et de courrier électronique Web. Or, les communications de ces acteurs ne sont pas couvertes par le champ actuel de la directive « vie privée et communications électroniques ». C'est donc à une équivalence fonctionnelle que procède ici la Commission européenne, afin de faire bénéficier les utilisateurs des télécommunications au sein de l'Union européenne d'une protection efficace et identique.

De plus, ainsi que l'ont exposé les membres du cabinet de M. Ansip, cette proposition de règlement vise à appliquer les principes de base que sont la sécurité et la confidentialité des télécommunications à un nouveau contexte technologique. C'est la prise en compte de cette dimension ainsi que de la jurisprudence de la CJUE qui ont conduit à appliquer ces principes aux métadonnées.

La Commission européenne présente cette proposition de règlement comme une *lex specialis* de RGPD, en ce qu'elle en précise certains aspects et en complète d'autres dans le domaine des télécommunications. Vos rapporteurs souhaitent souligner que les acteurs privés rencontrés lors des auditions ont été nombreux à soulever la « double peine » que constituait l'adaptation à la proposition de règlement, alors que la phase d'adaptation au RGPD ne sera véritablement terminée, pour les plus avancés d'entre eux, au 25 mai 2018. D'autre part, le texte pose des questions d'harmonisation avec le RGPD dans l'ensemble, soulevé notamment par les opérateurs économiques du domaine des télécommunications, qui pourraient poser la question de la sécurité juridique de l'ensemble. Les investissements effectués en vue de la conformité avec le RGPD doivent en effet être pérennes et ne pas être immédiatement biaisés en vertu de nouvelles réglementations.

2. Un texte fondé sur la notion de protection des données et du consentement

La proposition de règlement n'établit pas en elle-même de nouvelles obligations en matière de durée de la conservation des données, mais elle prend acte de la lecture combinée de la jurisprudence de la CJUE et de l'article 23 du RGPD. La CJUE a en effet consacré, lors de deux affaires différentes, le principe selon lequel la conservation des données personnelles ne peut se faire que de manière ciblée. La Cour a notamment estimé [(1)], que le droit en vigueur « s'oppose à une réglementation nationale prévoyant, à des fins de lutte contre la criminalité, une conservation généralisée et indifférenciée de l'ensemble des données relatives au trafic et des données de localisation de tous les abonnés et utilisateurs inscrits

(1) Arrêt de la Cour (grande chambre) du 21 décembre 2016, « Tele2 Sverige AB contre Post- och telestyrelsen et Secretary of State for the Home Department contre Tom Watson e.a. »

concernant tous les moyens de communication électronique. » La possibilité pour les métadonnées de révéler des informations sensibles et personnelles a en outre été explicitement reconnue. Cela explique la définition volontairement large utilisée par la Commission européenne : le règlement a vocation à s'appliquer, en toute neutralité technologique, à tout contenu transmis ou échangé et toute information concernant l'utilisateur final de services de communications électroniques traitée aux fins de la transmission, la distribution ou l'échange de ce contenu, y compris les données permettant de retracer une communication et d'en déterminer l'origine et la destination ainsi que le lieu, la date, l'heure, la durée, le type. Dès lors, toute métadonnée susceptible d'être relevée sur un réseau, dès lors qu'elle donne des informations sur l'émetteur ou le destinataire du contenu, doit connaître un niveau de confidentialité comparable à celui des autres contenus.

En cohérence avec la position de la CJUE, vos rapporteurs estiment que la conservation des données ne peut faire l'économie d'un encadrement strict, respectant les nécessités propres à la sécurité de l'État et à la lutte contre le terrorisme en particulier, mais n'excédant pas les moyens appropriés et proportionnés à ces objectifs. Les règles de confidentialité doivent donc s'appliquer tout autant aux informations échangées qu'aux éléments extérieurs à la communication lorsque ceux-ci informent sur la localisation, la date à laquelle les données ont été émises ou encore le destinataire de celles-ci.

La Commission a véritablement souhaité faire de cette *lex specialis* le pendant du RGPD dans un domaine spécifique, comme en témoigne l'attention portée à la notion de consentement. L'intérêt porté au traitement des données personnelles par le biais des télécommunications tient en effet au fait que le contenu des communications peut évidemment révéler des aspects relatifs aux questions de santé, de préférence sexuelle, d'opinion ou de croyance des utilisateurs et leur réemploi sans consentement préalable. Cette question concerne également les personnes morales dont les secrets d'affaires ou toute autre information sensible qui peut être échangée par le biais des télécommunications. Le projet de règlement constitue donc l'une des déclinaisons sectorielles du RGPD.

Le champ du consentement relatif aux données personnelles est ici défini de manière presque inconditionnelle : « toute interférence avec la transmission [de ces données] soit directement par intervention humaine, soit indirectement par traitement automatisé, sans le consentement de toutes les parties communicantes, devrait être interdite. »

La Commission, dans son examen REFIT, a estimé que le consentement de l'utilisateur final n'était pas obtenu de manière appropriée en ce qui concerne les témoins traceurs, ou cookies. L'acceptation est en particulier biaisée par les conditions dans lesquelles elle est demandée. L'utilisateur final est souvent dans une position qui ne lui permet pas de comprendre ce qu'est un cookie, parfois installé sans son consentement. Des associations comme la Quadrature du Net sont particulièrement sensibles à la question et 82 % des particuliers ayant répondu à la

consultation de la Commission européenne soutiennent la solution consistant à imposer aux fabricants d'équipements terminaux l'obligation de commercialiser des produits dotés de paramètres de confidentialité activés par défaut. Cette obligation est par ailleurs consacrée par l'article 25 du RGPD [(1)] . La proposition de règlement va même plus loin que le RGPD sur certains points, comme l'a relevé le BEUC (Bureau européen des unions de consommateurs) : il vise à protéger les consommateurs contre des communications commerciales non sollicitées.

La Commission européenne a toutefois pris conscience de l'impact d'une telle mesure sur les prestataires en ligne dont le financement vient avant tout de la publicité ciblée, à l'instar des éditeurs de presse, puisqu'elle reconnaît qu'il sera peut-être plus difficile aux annonceurs en ligne pratiquant le ciblage d'obtenir un consentement si une forte proportion d'utilisateurs choisit le paramètre « refuser les cookies de tiers ». De la même manière, « le fait, pour un fournisseur de services de la société de l'information, de vérifier une configuration afin de fournir un service conformément aux paramètres de l'utilisateur final, et de consigner simplement que le dispositif de celui-ci ne permet pas de recevoir le contenu demandé par l'utilisateur final ne devrait pas être considéré comme un accès audit dispositif ni comme une utilisation des fonctions de traitement du dispositif. »

Pour autant, la proposition de règlement privilégie l'option selon laquelle les navigateurs internet seraient les entités établissant la boîte de dialogue entre l'utilisateur qui a refusé les cookies et les sites Web qui proposent à l'internaute de revenir sur son choix, à des fins d'économies sur les coûts de mise en conformité. Il s'agit de faire en sorte que le choix fait par l'utilisateur dès l'installation de son navigateur en matière de confidentialité s'impose aux tiers et leur soit opposable. Si pour le moment le paramétrage par défaut des navigateurs consiste, la plupart du temps, à accepter tous les cookies, vos rapporteurs estiment qu'il est légitime que l'utilisateur puisse avoir accès à un large éventail de possibilité en matière d'acceptation des cookies, incluant les options les plus extrêmes de refus total ou d'acceptation totale. Ces options devraient aussi inclure la question des cookies de tiers.

---

(1) Article 25 du Règlement général de protection des données :

« 1. Compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, que présente le traitement pour les droits et libertés des personnes physiques, le responsable du traitement met en œuvre, tant au moment de la détermination des moyens du traitement qu'au moment du traitement lui-même, des mesures techniques et organisationnelles appropriées, telles que la pseudonymisation, qui sont destinées à mettre en œuvre les principes relatifs à la protection des données, par exemple la minimisation des données, de façon effective et à assortir le traitement des garanties nécessaires afin de répondre aux exigences du présent règlement et de protéger les droits de la personne concernée.

2. Le responsable du traitement met en œuvre les mesures techniques et organisationnelles appropriées pour garantir que, par défaut, seules les données à caractère personnel qui sont nécessaires au regard de chaque finalité spécifique du traitement sont traitées. Cela s'applique à la quantité de données à caractère personnel collectées, à l'étendue de leur traitement, à leur durée de conservation et à leur accessibilité. En particulier, ces mesures garantissent que, par défaut, les données à caractère personnel ne sont pas rendues accessibles à un nombre indéterminé de personnes physiques sans l'intervention de la personne physique concernée. »

II. LES POINTS DE VIGILANCE SUR CE TEXTE SONT NOMBREUX

A. LE RISQUE DE PÉNALISER LES INDUSTRIES DU NUMÉRIQUE, EN VOIE D'ADAPTATION AU RGDP

De nombreux acteurs privés entendus par vos rapporteurs les ont alertés quant aux risques que pouvait porter, pour leur activité, l'application de la proposition de règlement telle qu'elle était jusqu'à présent négociée.

1. Une nécessaire coordination avec le RGPD

La première inquiétude porte sur l'application simultanée du RGPD et du règlement *ePrivacy*. Même si, compte tenu des négociations actuelles, il devient très peu probable que ce dernier entre en vigueur au 25 mai 2018, en même temps que le RGPD, son champ d'application relativement large recoupe en partie celui du RGPD. Ainsi, les représentants de Microsoft, malgré leur capacité d'adaptation, ont indiqué à vos rapporteurs qu'il serait difficile, compte tenu des prévisions actuelles de la Commission européenne, de mettre en œuvre le règlement *ePrivacy* de manière efficace. Ainsi, « le calendrier, qui voudrait que ce texte soit applicable simultanément avec le Règlement général relatif à la protection des données (RGPD) au 25 mai 2018, est tout à fait illusoire au regard de l'état d'avancement de la procédure devant le Conseil. Et ce d'autant plus que les entreprises sont déjà fortement mobilisées par leur mise en conformité avec le RGPD, ce qui impose d'éviter toute redondance voire contradiction entre les deux textes. » Vos rapporteurs ont également été alertés sur les conditions dans lesquelles ont été lancées les négociations sur le texte. Il semble que les efforts de réflexion en amont qui avaient présidé à la construction du RGPD n'ont pas été répétés pour le projet de règlement *ePrivacy*. Malgré la discussion politique qui s'est tenue le 4 décembre au Conseil télécommunication, il est peu probable que le calendrier initial puisse être tenu, compte tenu des larges implications économiques qu'il pourrait avoir sur certains acteurs spécifiques.

Les articles 5 et 6 pourraient, selon une partie des personnes auditionnées, entraîner des difficultés technologiques. Le premier, qui porte sur la « confidentialité des données de communications électroniques » interdit par principe le traitement de toutes données de communication électroniques (métadonnées ou données de contenu) sans distinction, que celles-ci soient stockées ou en transit. Le second, relatif au « traitement autorisé des données de communications électroniques » instaure les exceptions à l'article 5, exceptions très restrictives et principalement basées sur le consentement des utilisateurs. Or, aujourd'hui, selon les représentants de Microsoft en particulier, ces dispositions pourraient empêcher un fonctionnement optimal d'outils tels que les assistants personnels intelligents, destinés à traiter des données en transit au sein de mails, entre autres. De la même manière, la récolte du consentement auprès de *tous* les utilisateurs, ayant souscrit ou non au service de communication, pourrait entraîner de lourdes charges sur les services de communication. Dans le cas d'une

application permettant de lire vocalement les messages pour les handicapés, il s'agirait d'identifier les expéditeurs de chaque message, et de parvenir à solliciter leur consentement pour le traitement de leur message par l'opérateur du service d'assistant personnel.

À l'inverse, l'article 11 du projet de règlement a contribué à l'inquiétude d'associations de défense des internautes, à l'instar de la Quadrature du Net. L'extension des exceptions au principe de confidentialité des communications, outre la défense, la sécurité publique, les enquêtes et la poursuite des infractions, à la notion d'intérêt économique et financier, incluant des questions monétaires, budgétaires et fiscales, ainsi que la sécurité sociale et la santé, dépassent ce qui relève, pour vos rapporteurs, de la stricte nécessité. Plus largement, la confidentialité des données de communication doit passer par des modalités techniques destinées à assurer la plus grande protection possible contre toute forme d'intrusion, y compris de la part des autorités publiques. Seul un tel degré de chiffrement, connu sous le nom de « chiffrement de bout en bout », peut garantir un usage proportionné et soumis à la condition expresse d'une menace grave et immédiate à la sécurité publique de déchiffrement du contenu des télécommunications.

2. Les mécanismes de chiffrement doivent protéger efficacement les données de communication

Il est incontestable que les nouvelles formes de communication et d'organisation numériques peuvent accroître les difficultés auxquelles se heurtent les acteurs de la sécurité publique, en particulier en matière de lutte contre le terrorisme. Ce constat ne doit pourtant pas occulter le fait que, de la même manière qu'il n'existe pas de risque zéro, la recherche de la sécurité absolue est une gageure. Dès lors, il s'agit plutôt, pour vos rapporteurs, de viser un degré de sécurité suffisant pour permettre un exercice aussi large que possible des libertés fondamentales.

Le chiffrement des données et les messageries sécurisées constituent un point de cristallisation dans ce débat sur l'équilibre entre sécurité et liberté. Il est bien souvent affirmé que les solutions de chiffrement, notamment « de bout en bout », constituent un obstacle à l'efficacité des forces de l'ordre dans la prévention d'une attaque terroriste, et mettent donc en péril la sécurité des citoyens. Dans cette logique, la solution serait, pour certains, de contraindre les constructeurs et fournisseurs de logiciels à installer des *backdoors* dans leurs systèmes, auxquelles seuls les services de renseignement auraient accès.

Or, rien n'est plus dangereux pour les utilisateurs et il n'est nullement garanti que cette solution permette un gain d'efficacité en matière de sécurité intérieure :

- d'une part, la multiplication des cyberattaques vient rappeler régulièrement que l'affaiblissement volontaire d'un programme ou

d’un service en ligne fait courir un risque substantiel pour la sécurité des utilisateurs ;

- d’autre part, des stratégies de contournement ne manqueront pas d’être mises en œuvre par les organisations criminelles, dès lors qu’il est aujourd’hui de plus en plus aisé de développer un logiciel non contrôlable, facile à distribuer et qui comporte un très fort niveau de sécurité.

En substance, ainsi que l’indique le CNNum dans son avis de septembre 2017, « il n’existe pas de technique d’affaiblissement systémique du chiffrement qui ne permettrait de viser que les activités criminelles. Limiter le chiffrement pour le grand public reviendrait alors à en accorder le monopole aux organisations qui sauront en abuser ».

Il convient donc d’accorder la plus grande vigilance à ce que les garanties de sécurité apportées par le chiffrement, ainsi que son importance dans la protection de la vie privée, ne soient pas remises en cause au nom de solutions contre-productives.

À l’inverse, des solutions existent déjà pour permettre l’obtention d’informations nécessaires au bon déroulement d’une enquête. Elles méritent d’être mises en avant : exploitation des failles techniques, piratage du terminal mobile, analyse des métadonnées pour cartographier un réseau ou localiser des individus.

B. DES MODALITÉS À PRÉCISER POUR QUE LES OBJECTIFS LÉGITIMES NE PÉNALISENT PAS INDÛMENT LES ACTEURS ÉCONOMIQUES

1. Le champ d’application de la proposition de règlement

Vos rapporteurs souhaitent également souligner le fait que le projet de règlement introduit des distorsions économiques auxquelles les personnes auditionnées ont souvent fait référence. Malgré l’inclusion d’acteurs dits OTT dans le champ d’application de la directive, il demeure des disparités techniques susceptibles de désavantager les acteurs traditionnels. C’est ainsi qu’il maintient des obligations strictes pour les seuls « réseaux de communications électroniques », notion qui n’inclue pas les services transitant par d’autres voies, comme le GPS ou les échanges directs entre machines. Ainsi, selon le considérant 17 de la proposition de règlement, « les données de localisation qui sont générées dans un contexte autre que celui de la fourniture de services de communications électroniques ne devraient pas être considérées comme des métadonnées. »

De plus, la proposition de règlement *ePrivacy* peut donner à certains de ces acteurs le sentiment d’une « double peine », notamment dans le domaine des télécommunications. Le président de l’ARCEP a mentionné la difficulté de se conformer à une double réglementation, dont les champs d’application peuvent

parfois se recouper, ce qui créé des effets d'insécurité juridique potentiellement préjudiciables. Les représentants d'Orange estimaient également qu'il serait « contre-productif que le règlement *ePrivacy* en préparation maintienne des spécificités sectorielles contradictoires avec le RGPD, alors même que les entreprises auront déjà mis en place les moyens nécessaires à son application au niveau national. »

Le champ d'application du règlement concerne notamment, ainsi qu'il est établi dans le considérant 12, l'Internet des objets. Ces objets connectés fonctionnent en grande partie en M2M, soit la communication de machine à machine, ce qui implique la transmission de signaux sur un réseau et nécessite donc un service de communication électronique. Le règlement permet d'appliquer le principe de confidentialité à ces acteurs également. Plusieurs acteurs du numérique, à l'instar d'IBM, par exemple, ont alerté vos rapporteurs sur les difficultés que cette application pouvait présenter. En effet, si une demande de consentement s'applique à chaque opération d'un objet connecté, ce système pourrait diminuer fortement la valeur ajoutée de ce type d'objet, voire en entraver le fonctionnement. L'impossibilité d'identification des utilisateurs finaux dans de nombreux cas empêcherait de recueillir leur consentement et de pouvoir procéder à un traitement des données à des fins analytiques. Un grand nombre de dispositifs M2M s'en trouveraient entravés dans leur fonctionnement. De la même manière, le passage d'une économie fondée sur des données descendantes à l'utilisation de données montantes complique le bon fonctionnement de la proposition de règlement *ePrivacy*. Pour les représentants d'IBM, il conviendrait donc d'avoir une approche sectorielle qui distingue, en fonction des technologies, les modalités de recueil du consentement, notamment en ce qui concerne l'internet des objets.

2. Le consentement en matière de traceurs

La principale question porte toutefois sur l'application du consentement aux acteurs numériques qui fondent leur économie sur l'usage de la publicité ciblée, fondée sur des traceurs tiers, ou « *cookies* ». En effet, le vote par la Commission LIBE du rapport de Mme Lauristin en octobre 2017 a renforcé les exigences de consentement en la matière, puisque le considérant 18 dispose désormais que « le consentement ne devrait pas être considéré comme libre s'il est requis pour accéder à un service ou obtenu par des demandes répétées. Pour éviter de telles demandes abusives, les utilisateurs devraient être en mesure d'exiger des fournisseurs de services qu'ils se souviennent de leur refus et qu'ils se conforment à des spécifications techniques signalant le refus, le retrait du consentement ou une objection. » La rapporteure a été particulièrement attentive à la nécessité de préserver le caractère libre et éclairé du consentement en matière de traceurs, à l'instar de ce que prévoit le RGPD. Des associations telles que le BEUC ont soutenu cette position, en estimant que l'alignement avec le RGPD aboutirait à une ambition moindre dans la protection du consommateur sur internet. De manière plus spécifique, les membres du Parlement européen ont demandé à ce que soient bannies les pratiques des bandeaux d'annonce des cookies. Enfin, ils

ont élargi le champ d'options à la disposition de l'utilisateur de la manière suivante. Les fournisseurs de logiciels de type navigateurs doivent proposer l'acceptation de cookies distincts selon leur finalité :

- un suivi à des fins commerciales ou à des fins de prospection directe à des fins non commerciales (publicité comporte-mentale) ;

- un suivi aux fins de la fourniture de contenu personnalisé ;

- un suivi à des fins d'analyse ;

- un suivi des données de localisation ;

- la communication de données à caractère personnel à des tiers.

Enfin, au moment de la première utilisation ou de l'installation du navigateur, les utilisateurs devraient, selon le rapport de Mme Lauristin, être informés de la possibilité de modifier les paramètres de confidentialité par défaut pour choisir l'option qui leur convient le mieux. Les représentants de Qwant ont notamment exprimé leur satisfaction par rapport à ce système. De la même manière, les représentants du BEUC ont demandé à vos rapporteurs de ne pas s'appuyer sur le principe de « l'intérêt légitime » des acteurs privés dans le traitement des données personnelles. L'insertion d'une telle mention pourrait, selon eux, abaisser le niveau de protection des données personnelles à un niveau inférieur à celui qui était garanti sous le régime de la directive de 2002 [(1)].

Toutefois, de telles modalités de recueillement du consentement pourraient nuire à des pans entiers de l'économie numérique, à commencer par les éditeurs de presse. Les quotidiens nationaux recueillent en effet aujourd'hui la majorité de leur lectorat sur internet. Ainsi, en janvier 2017, sur 39 millions de lecteurs, les quotidiens nationaux comptaient 84 % de lecteurs numériques, dont 38 % ne lisent le journal qu'en ligne. Selon les projections d'une étude commandée en 2017, 52 % des revenus de ces quotidiens nationaux en France seront issus du numérique en 2020 et 100 % des revenus publicitaires proviendraient alors d'annonces liées aux données des utilisateurs. La mise en place du règlement à l'heure actuelle viendrait remettre fortement en cause le modèle de la publicité ciblée sur lequel s'appuient actuellement les éditeurs de presse, en raison d'un très grand taux de refus des cookies. La même étude estime que si le taux d'acceptation des cookies sur les sites des éditeurs de presse est aujourd'hui de 95 %, il tomberait à 13 % après la mise en application du règlement. Une telle chute se traduirait par une réduction des revenus numériques des quotidiens nationaux de 57 %, due notamment à la diminution de la croissance des revenus liés aux contenus et à une perte de revenus sur la publicité programmatique [(2)].

---

(1) Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques)

(2) Syndicat de la Presse Quotidienne Nationale. Étude d'impact du projet de règlement ePrivacy, 27 Juillet 2017

Une étude a été initiée à l'initiative du Ministère de la Culture, du Ministère des Finances et du Secrétaire d'État au Numérique, afin d'évaluer objectivement l'impact de ce projet de règlement sur l'ensemble du secteur.

Cette opinion est également partagée par d'autres acteurs tels que les entreprises de télécommunication. Orange a ainsi précisé que le projet de règlement ne permet notamment pas le traitement des métadonnées sur les fondements de l'« intérêt légitime », de l'« exécution du contrat » ou du « traitement ultérieur compatible », alors que ces notions sont retenues comme base pour le traitement des données personnelles par les textes nationaux et européens, y compris le RGPD. Ainsi, aux termes de l'actuel projet de règlement, le traitement des métadonnées, contrairement à celui des données personnelles, reposerait exclusivement sur le consentement, alors même que la multiplication des demandes systématiques de consentement a montré son inadéquation dans l'univers numérique.

Enfin, la gestion du consentement au niveau des navigateurs pourrait leur donner un avantage concurrentiel certain alors même que la plupart des navigateurs utilisés par les internautes européens n'appartient pas à des sociétés européennes. Google Chrome, par exemple, autorise déjà l'utilisateur à user de nombreuses options quant à l'acceptation des cookies.

À la lumière de ces analyses divergentes, vos rapporteurs estiment qu'il convient de trouver des solutions qui permettent aux internautes d'exercer leur droit d'exprimer le consentement libre, spécifique, éclairé et univoque au traitement des données.

Vos rapporteurs estiment par ailleurs que, sur internet, l'anonymat n'est jamais réellement possible. Les habitudes de navigation des utilisateurs font l'objet d'une analyse fine, souvent via l'utilisation de cookies ou d'autres traceurs (*fingerprinting, web bugs*). Les cookies tiers sont notamment partagés par plusieurs sites et constituent un risque en termes de sécurité pour l'utilisateur, via le *data leakage*. La confiance dans le numérique est une question centrale pour son développement, or l'absence de consentement libre et éclairé sur les traceurs l'entache.

Depuis 2009, le dépôt des cookies est soumis au consentement de l'utilisateur. Ce consentement est loin de constituer un consentement éclairé mais demeure principalement formel. Aujourd'hui, les utilisateurs se voient imposer un dépôt obligatoire des cookies, puisque seulement un très faible nombre d'entre eux fait réellement l'effort d'évaluer l'étendue des informations transmises. Bien souvent, ils se contentent d'accepter passivement le dépôt des cookies pour accéder au service. S'ils changent d'avis, les utilisateurs ne peuvent agir qu'après le dépôt en supprimant ces cookies. Il est donc essentiel, voire urgent, de redéfinir la notion de consentement pour que son effectivité soit véritablement garantie.

Il est évident que les traceurs constituent un outil de surveillance de l'utilisateur à des fins commerciales, sans que l'utilisateur lui-même ne soit informé quant au traitement des données recueillies ou leur durée de conservation. Certains médias en ligne sont aujourd'hui fortement dépendants de la publicité ciblée dans leur modèle économique. Il convient donc de prendre en compte les conséquences que peut emporter l'application du consentement des utilisateurs finaux sur leur développement, une conception trop extensive de cette application pouvant entraîner une chute drastique du nombre d'internautes consultant les sites de la presse en ligne.

La proposition avancée par la Commission européenne est donc insuffisante en l'état. Centraliser le consentement des utilisateurs au moyen des paramètres de confidentialité de leur navigateur internet, ne permet pas, pour vos rapporteurs, un consentement libre et éclairé. De plus, la concentration des rôles d'éditeur de navigateur définissant les paramètres de confidentialité, d'émetteur de cookie, et de régie publicitaire au sein d'un acteur unique comme Google, n'est pas sans susciter d'interrogations sur sa neutralité et sa conformité au droit de la concurrence.

À l'inverse, nous ne devons pas présumer le consentement par un réglage prédéfini, mais exiger que le navigateur avertisse l'utilisateur à chaque dépôt de cookie tiers ou de pistage supplémentaire. Comme le soulignent les représentants de Qwant, le dépôt d'un cookie ne doit pas être présumé via un réglage prédéfini du navigateur : « Les Européens devraient toujours donner un consentement libre, explicite, spécifique et éclairé, lorsque des entreprises souhaitent collecter leurs données et les tracer sur Internet ».

DEUXIÈME PARTIE : LA LIBRE CIRCULATION DES DONNÉES A CARACTÈRE NON PERSONNEL

I. L'ESSOR DE L'ÉCONOMIE DU NUMÉRIQUE ABOUTIT À LA MULTIPLICATION DE L'UTILISATION DES DONNÉES

A. ENCADRER LES ÉCHANGES DE DONNÉES NON PERSONNELLES : UNE NÉCESSITÉ

L'Union européenne a initié une législation encadrant les services, relativement complète depuis la mise en place du marché intérieur. Entre autres, la directive « Services »[1] instaure la liberté d'établissement des prestataires de services dans n'importe quel État membre. Elle contient certes des exceptions et son champ d'application met de côté en particulier certains services de commerce électronique. Auparavant, la directive sur le commerce électronique de 2000[2] avait établi la libre circulation des services de la société de l'information, sans toutefois spécifiquement traiter des données.

Ainsi, dans le domaine de l'économie numérique, aucune règle précise ne s'applique si ce n'est les dispositions générales du traité sur le Fonctionnement de l'Union européenne. Lorsque les fournisseurs de services ou les entreprises clientes rencontrent des problèmes pour exercer librement leur activité dans un État membre, la gestion du conflit s'effectue donc au cas par cas par des procédures d'infraction envers tel ou tel État membre. C'est pourquoi la Commission européenne a relevé une faiblesse face aux obstacles au sein du marché intérieur. La seule invocation des articles 49 et 56 du traité sur le Fonctionnement de l'Union européenne ne semble pas satisfaisante économiquement et en matière de protection et droits des utilisateurs. Ce manque est notamment dû au fait que lors de l'adoption des directives sur les services et le commerce électronique, les technologies présentes sur le marché n'étaient pas les mêmes qu'actuellement. En particulier, les services de stockage ou de traitement des données n'étaient pas aussi fondamentaux et répandus.

Il existe un faible nombre de règles encadrant les données en tant que telles. La directive sur les bases de données[3], notamment issues de machines

---

[1] *Directive 2006/123/CE du Parlement européen et du Conseil du 12 décembre 2006 relative aux services dans le marché intérieur*

[2] *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*

[3] *Directive 96/9/CE du Parlement européen et du Conseil du 11 mars 1996 sur la protection juridique des bases de données*

industrielles, empêche la réutilisation de données ayant été obtenue grâce à un investissement substantiel. De même, la directive sur les secrets d'affaires[1], qui doit être transposée avant juin 2018, protège les données qui s'apparentent à un secret d'affaires dans la mesure où elles peuvent être identifiées comme participant du capital intellectuel de l'entreprise. Les données personnelles sont encadrées par deux directives : celle de 1995[2] qui tend à garantir le respect de la vie privée mais aussi à faciliter la libre circulation de ces données, et celle de 2002[3] qui renforce les règles dans le domaine des communications électroniques. Au niveau national, les données non personnelles ne sont protégées que dans le cadre limité du droit de propriété intellectuelle ou du secret d'affaires. Ainsi, il est clair que la législation actuelle n'est pas adaptée à l'accroissement de l'utilisation des données non personnelles dans l'économie numérique.

B. LE CONSTAT D'UNE ÉCONOMIE EN PLEINE EXPANSION MAIS RALENTIE PAR UN CERTAIN NOMBRE D'OBSTACLES

L'économie des données représente une opportunité non-négligeable pour stimuler la croissance au sein de l'Union européenne. La Commission européenne, lors de la présentation de sa proposition pour créer une économie européenne numérique[4], en janvier 2017, a indiqué qu'en 2015, les données représentaient une valeur estimée de 272 milliards d'euros, soit environ 1,9 % du PIB européen. L'économie numérique pourrait doubler de valeur, selon la Commission européenne, grâce à la libre circulation des données pour atteindre 4 % du PIB en 2020[5].

Les données sont au centre de domaines variés de l'économie et vont devenir un élément central pour de nombreuses entreprises, de manière exponentielle. L'économie des données s'est transformée via des innovations technologiques telles que les services en nuage, l'intelligence artificielle ou les objets connectés. Les acteurs privés auditionnés tout comme le CNNum ont exposé le fait que la circulation des données était incontournable puisqu'elle constitue la base de fonctionnement d'Internet et des activités économiques qui en dépendent. Ainsi, sont concernés tout aussi bien les domaines de la santé, des objets intelligents ou encore de la protection civile que les secteurs plus traditionnels comme l'énergie ou l'agriculture. Les données forment une « matière

---

[1] *Directive 2016/943/UE du Parlement européen et du Conseil du 8 juin 2016 sur la protection des savoir-faire et des informations commerciales non divulgués (secrets d'affaires) contre l'obtention, l'utilisation et la divulgation illicites*

[2] *Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données*

[3] *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*

[4] *Commission européenne. Communication « Créer une économie européenne fondée sur des données » du 10 janvier 2017, COM(2017) 9*

[5] *Commission européenne. Fiche d'information sur l'État de l'Union 2017 à propos de la libre circulation des données publiée le 20 septembre 2017.*

première » de qualité pour encourager la recherche et l'innovation. Notamment, l'utilisation des données de consommation permet de mieux réguler la fourniture d'énergie, via des compteurs intelligents, ou d'anticiper les besoins en infrastructure dans l'industrie. Par exemple, l'analyse des données de machines dans une usine peut permettre de connaître de manière précise l'état de fonctionnement du matériel et donc d'anticiper le rachat ou la réparation d'outils défaillants. La Commission européenne, dans cette perspective, a créé un incubateur de données ouvertes, ODINE, afin de faciliter l'accès à des données ouvertes pour les PME et stimuler ainsi la valeur ajoutée et l'innovation. L'usage des données dépend toutefois de technologies sans cesse en développement. Cela rend d'autant plus complexe la régulation d'un domaine déjà large.

La Commission européenne a toutefois constaté la présence de certains obstacles au sein du marché intérieur européen qui entravent le potentiel de développement d'une économie basée sur les données, lors de sa consultation publique sur la construction d'une économie européenne des données menée en 2017[1]. Ces obstacles empêcheraient, selon la Commission européenne, non seulement la libre circulation des données transfrontalière mais aussi entre les plateformes :

- Les législations nationales restreindraient dans certains États membres la localisation des données. Cela a un impact économique certain, dans la mesure où l'obligation de localisation des données sur un territoire précis rend plus difficile et plus coûteuse la commercialisation de produits ou de services utilisant les données non personnelles dans plusieurs pays. Les entreprises sont obligées, en cas de restriction, de disposer de serveurs de stockage des données dans chacun des États membres dans lesquels elles opèrent et donc de dupliquer leurs systèmes. Dans certains cas, ce blocage géographique peut être justifié, en matière de santé notamment. Certaines réglementations peuvent toutefois être disproportionnées, selon l'analyse de la Commission européenne ; ainsi, le stockage national des archives du secteur public serait trop peu accessible, même lorsque les données ne possèdent aucun caractère sensible. C'est le cas notamment aux Pays-Bas comme l'a précisé la DG JUST de la Commission européenne lors de son audition ;

- Les obstacles ne sont pas uniquement réglementaires mais peuvent aussi être liés à des caractéristiques techniques ou contractuelles. La Commission européenne souligne le problème d'interopérabilité des données : l'échange de données ne peut être effectif à cause de normes techniques différentes entre les plateformes, par exemple le format des données peut ne pas être

[1] *Commission européenne. Consultation publique menée entre le 10 janvier et le 26 avril 2017 et publiée le 31 mai 2017 sur la construction d'une économie européenne des données*

supporté par le système d'un autre fournisseur de services numériques. Il convient donc de réfléchir à l'adoption de normes sectorielles. La CSNP (Commission Supérieure du Numérique et des Postes) a parlé d'un « protectionnisme d'État » dans certains pays. Dans certains cas, la faible portabilité des données entre les plateformes de stockage en nuage peut nuire à la concurrence. En effet, il n'y a aucune obligation juridique pour permettre la portabilité des données. Ce droit est donc institué lors de la signature des contrats entre le fournisseur et le client, au cas par cas. Cela peut être défavorable aux entreprises lorsqu'elles se retrouvent en position de faiblesse lors de la rédaction des contrats avec les fournisseurs de service ;

- L'insécurité juridique liée à la fragmentation du droit relatif aux données au sein du marché intérieur complique l'activité des entreprises. En particulier, le syndicat SYNTEC Numérique a insisté sur le coût et la perte de temps pour les entreprises si celles-ci doivent analyser le droit national de tous les États membres dans lesquelles elles exercent leur activité. De même, les auditions ont permis à vos rapporteurs d'appréhender la peur de certains acteurs publics ou privés quant à la confidentialité des données non personnelles qu'ils sont amenés à utiliser. ;

- Les risques de sécurité concernant l'accès transfrontalier aux données aboutissent à une diminution de la confiance des acteurs privés exerçant une activité transfrontalière et ne stimulent pas l'utilisation de lieu de stockage en dehors du pays d'activité.

II. LA CRÉATION D'UN MARCHÉ INTÉRIEUR DU NUMÉRIQUE DOIT PASSER PAR LA RECONNAISSANCE DE LA LIBERTÉ DE CIRCULATION DES DONNÉES NON PERSONNELLES

La Commission européenne, dans la continuité de sa stratégie pour un marché unique du numérique, a présenté le 13 septembre 2017, une proposition de règlement afin de mettre en place un cadre réglementaire pour la libre circulation des données à caractère non personnel[1]. Les mesures développées dans cette proposition avaient déjà été évoquées partiellement dans une communication de la Commission européenne visant à « créer une économie européenne fondée sur les données » en janvier 2017[2].

Le domaine de l'économie des données est défini de manière large par ledit règlement. Le champ d'application concernerait le stockage ou le traitement des données d'un utilisateur européen ou par un fournisseur établi dans un État membre. Les données à caractère non personnel sont caractérisées de manière exclusive en précisant que ce sont celles qui ne sont pas concernées par l'article 4, paragraphe 1 du RGPD. En d'autres termes, ce sont donc toutes les données ne permettant pas d'identification directe ou indirecte de l'utilisateur.

Cette question de la définition du périmètre des données non personnelles demeure toutefois cruciale pour vos rapporteurs. La mise en œuvre efficace de l'harmonisation des normes pour encourager la circulation des données mais aussi la cohérence avec les textes encadrant le régime des données personnelles reposent sur une définition précise et une interprétation unique par l'ensemble des États membres. Cet enjeu a ainsi été abordé lors des auditions, puisque des associations comme la Quadrature du Net ont exprimé un certain scepticisme devant la faiblesse de la définition utilisée par la Commission européenne. Les mécanismes de pseudonymisation en particulier peuvent certes être employés avec profit pour compliquer la « remontée » vers l'utilisateur initial. Toutefois, il semble à vos rapporteurs que seule une anonymisation véritable empêchant de rendre à nouveau personnelles les données doit être autorisée afin de protéger l'utilisation de ces dernières. Les représentants de Qwant ont en effet fait part à vos rapporteurs de la difficulté d'être certain que les données soient anonymisées de manière irrévocable.

Le CNNum soutient quant à lui que la définition de données non personnelles ne peut pas être large, afin de protéger les actifs cruciaux des entreprises. Seules les données fournies par le consommateur directement doivent entrer dans le champ d'application du règlement. Le savoir-faire des entreprises

---

[1] *Proposition de règlement du Parlement européen et du Conseil concernant un cadre applicable à la libre circulation des données à caractère non personnel dans l'Union européenne, COM(2017) 495*

[2] *Commission européenne. Communication « Créer une économie européenne fondée sur des données » du 10 janvier 2017, COM(2017) 9*

associé aux données lors du traitement de celles-ci, relève du domaine des données propres à l'entreprise et leur valeur doit donc être reconnue.

A. AMÉLIORER LA MOBILITÉ DES DONNÉES POUR UN MARCHÉ UNIQUE EFFICACE

L'harmonisation des règles concernant la libre circulation des données à caractère non personnel établirait un principe d'unicité au sein du marché intérieur. Cela mettrait fin à l'insécurité juridique évoquée ci-dessus. Cette nouvelle liberté de circulation, que d'aucuns considèrent comme une potentielle « cinquième liberté » au sein du marché intérieur, est d'autant plus essentielle qu'il existe une croissance exponentielle des produits et services digitalisés.

Les États membres auront, sous ce régime, l'obligation de supprimer toute réglementation instaurant des restrictions injustifiées de localisation pour le stockage ou le traitement des données. Seules pourraient être justifiées et proportionnelles les mesures relevant explicitement de la sécurité publique. Afin de garantir le respect de ce principe, la proposition de règlement prévoit que les États membres devront notifier toute nouvelle mesure ayant pour objet une localisation des données justifiée et supprimer les règles non conformes au règlement. Cette notification reposera sur le principe de la directive de 2015 instaurant une procédure d'information pour toute nouvelle norme technique ou réglementaire dans le domaine de l'information[1].

Du point de vue économique, la libre circulation des données donnerait la possibilité aux entreprises de maximiser leur profit en localisant leur système de stockage des données là où le rapport coût bénéfice serait le plus rentable. Cela avantagerait en particulier les PME et les nouvelles entreprises qui accéderaient plus facilement à un marché plus large que celui des seuls utilisateurs nationaux comme plusieurs acteurs privés auditionnés, européens ou non, tels que Microsoft ou SYNTEC Numérique, l'ont souligné. Les barrières réglementaires pénalisent en effet davantage les entreprises de faible envergure qui ne bénéficient pas de l'expertise juridique ou des moyens financiers pour s'adapter à la fragmentation réglementaire actuelle. Outre la croissance rapide de ces entreprises, une plus grande circulation des données soutiendrait aussi l'innovation. Des règles harmonisées favoriseraient également l'utilisation, par les acteurs publics, de moyens dématérialisés. D'autre part, sur le plan environnemental, la Commission européenne a souligné le fait que passer par l'informatique en nuage plutôt que d'utiliser son propre système, pour une petite entreprise, réduirait ses émissions de carbone de plus de 90 %[2].

---

[1] *Directive (UE) 2015/1535 du Parlement européen et du Conseil du 9 septembre 2015 prévoyant une procédure d'information dans le domaine des réglementations techniques et des règles relatives aux services de la société de l'information*

[2] *Commission européenne. Communication « Créer une économie européenne fondée sur des données » du 10 janvier 2017, COM(2017) 9*

La libre circulation des données non personnelles est un élément essentiel à la cohérence du droit européen. Elle complète de manière substantielle le Règlement de protection des données qui entrera en vigueur le 25 mai 2018 et traite des données personnelles uniquement.

B. FACILITER LA PORTABILITÉ DES DONNÉES POUR UN MARCHÉ CONCURRENTIEL

Il conviendrait par ailleurs de faciliter la concurrence entre les services de nuage informatique, afin à la fois de baisser les coûts et de stimuler l'innovation en la matière. L'Union bénéficie en effet de nombreux acteurs particulièrement actifs dans ce domaine, à l'instar d'OVH, qui pourraient dès lors étendre leurs activités à l'échelle du marché européen. Les nuages informatiques ne connaissant pas mieux les frontières que les nuages physiques, il serait illusoire de se retrancher en la matière derrière une forme de « ligne Maginot » nationale. Le partage de données non personnelles au sein de l'Union paraît donc fondamental pour le développement de ce secteur.

En vertu d'un réel droit à la portabilité de leurs données, les acteurs économiques pourraient comparer les différents services et opter pour celui qui correspond au mieux à leurs besoins en termes d'efficacité et de tarif. La Commission européenne a ainsi estimé que la baisse des coûts liée aux services de données pourrait contribuer à une hausse de huit milliards d'euros par an du PIB européen[1].

La régulation des fournisseurs de services en nuage s'effectuerait par le biais de codes de conduite autorégulateurs. Ces codes devront contenir des exigences en matière d'information des utilisateurs quant à la possibilité de se tourner vers un autre fournisseur, afin d'assurer la bonne infirmation des citoyens. C'est dans la même perspective que les fournisseurs auraient une obligation de transparence de leurs conditions d'utilisation. Les fournisseurs de services en nuage devront se coordonner afin de mettre fin à toute caractéristique technique qui rendrait impossible le rapatriement des données vers l'entreprise ou l'envoi de celles-ci vers un autre fournisseur. C'est à cette seule condition que l'on pourra réellement parler de portabilité des données. Ils devront aussi assurer une charge non excessive lors du transfert des données. Toutes ces mesures devront être mises en place dans un délai assez court puisque la Commission européenne s'engage à évaluer la mise en œuvre au plus tard deux ans après l'entrée en vigueur du règlement.

Vos rapporteurs estiment qu'il s'agit d'une des valeurs ajoutées réelle de cette proposition de règlement, compatible avec l'achèvement du marché unique du numérique sur ce sujet.

---

[1] *Commission européenne. Fiche d'information sur l'État de l'Union 2017 à propos de la libre circulation des données publiée le 20 septembre 2017.*

C. CONSERVER LES ACCÈS DES AUTORITÉS : POUR UN MARCHÉ SÉCURISÉ

La sûreté au sein de l'Union européenne demeure l'une des priorités de la Commission Juncker[1]. La libre circulation des données ne doit pas entraver la possibilité pour les autorités nationales d'accéder à celles-ci, en cas de nécessités liées notamment aux questions de sécurité nationale, mais aussi en vertu d'un intérêt public légitime. Les autorités concernées par l'accès aux données peuvent être celles qui effectuent des contrôles de conformité aux règles, comme lors d'une inspection ou d'un *audit*, mais aussi celles qui exercent une forme de surveillance pour assurer la sécurité des données. Ainsi, le règlement imposerait une coopération renforcée entre les États membres afin que cet accès soit garanti. De même, les entreprises continueront à devoir fournir leurs données lors d'un contrôle réglementaire. Ces mesures répondent ainsi à la crainte des États membres de voir leur contrôle de la sécurité diminuer, dès lors que les données auxquelles ils doivent avoir accès sont stockées dans un autre État membre.

Dès lors, des points de contact devraient être désignés au niveau de chaque État membre. Ils constitueront l'acteur unique pour servir d'interface avec les autres points de contact et la Commission européenne. Cela renforcera l'application effective des règles européennes concernant les données. L'assistance mutuelle sera rendue obligatoire afin de seconder les autorités d'un autre État membre lorsque celles-ci auront épuisé tous leurs moyens internes. Pour des raisons d'efficacité, ces points de contact devront être dotés des moyens suffisants pour remplir leurs tâches.

Par ailleurs, les règles en vigueur concernant la sécurité des données resteront applicables aux entreprises malgré la localisation des données dans un autre État membre. Il en est de même si les entreprises délèguent le traitement ou le stockage à des fournisseurs de services en nuage. Il s'agit là d'un prérequis indispensable afin d'assurer l'équilibre entre le fonctionnement du marché intérieur et la préservation de la souveraineté des États membres, dès lors que ces données peuvent avoir un rapport direct avec leurs activités régaliennes ou concerner immédiatement la sécurité des citoyens.

D. RÉFLÉCHIR À D'AUTRES INTIATIVES À L'AVENIR POUR COMPLÉTER LE MARCHÉ UNIQUE DU NUMÉRIQUE

Dans sa communication à propos de l'économie fondée sur les données[2], la Commission européenne a émis d'autres principes pour des mesures à prendre dans le futur.

---

[1] *Commission européenne. Discours sur l'État de l'Union prononcé par Jean-Claude Juncker le13 septembre 2017 devant le Parlement européen à Strasbourg.*

[2] *Commission européenne. Communication « Créer une économie européenne fondée sur des données » du 10 janvier 2017, COM(2017) 9*

La libre circulation des données non personnelles devrait entraîner un accès plus simple à celles-ci. L'amélioration du partage et de la réutilisation de ces données serait profitable à l'innovation et donc à la création de valeur au sein de l'Union européenne. En particulier, dans le domaine de la recherche, le volume de données produites par des machines ou des objets connectés croissant sans cesse, l'utilisation de larges volumes de données peut être indispensable. Dans ce but, la Commission européenne souhaite mettre en place un dialogue par le biais de consultations avec les acteurs industriels pour inciter au partage de données et à la création de nouveaux instruments technologiques afin d'exploiter pleinement le potentiel économique des données collectées. La confiance nécessaire pour faciliter la réutilisation des données amène aussi à agir sur le plan de la protection des investissements et des actifs. Favoriser l'innovation par le partage de données ne doit pas nuire aux investisseurs et donc un outil devrait leur garantir un juste retour, sur le modèle de ce qui peut se faire en matière de propriété intellectuelle. Vos rapporteurs ont en effet acquis la conviction, notamment en auditionnant des acteurs français et européens du numérique, que la maîtrise d'un large ensemble de données, à l'heure des plateformes, est un atout essentiel dans la concurrence mondiale actuelle. Le marché européen des données, qui se compose de 500 millions d'utilisateurs connectés efficacement, avec un fort pouvoir d'achat et une forte interactivité, représente une opportunité considérable. Les acteurs européens qui continuent à émerger, à l'instar de Qwant, mais aussi les futures entreprises d'objets connectés ou d'intelligence artificielle, y compris dans le domaine de la santé, doivent pouvoir bénéficier de volumes de données conséquents.

Enfin, l'Internet des objets soulève de nouveaux enjeux en matière de responsabilité. L'interconnexion entre les différents objets et le dialogue de machine à machine, ou M2M, amène à construire des systèmes complexes. Ainsi, en cas d'incident, il sera plus difficile d'identifier quel objet a été défectueux et donc qui est responsable. De telles problématiques sont particulièrement prégnantes pour ce qui est des voitures connectées, par exemple. Cela entraîne une insécurité juridique qui freine la conception et l'utilisation des tels objets. La Commission européenne voudrait donc établir un régime clair de responsabilité, fondé ou non sur la responsabilité actuelle du fait des produits défectueux[1]. Ce nouveau régime pourrait être complété par un nouveau type d'assurance, volontaire ou non, afin de garantir la protection des consommateurs.

[1] *Directive 85/374/CEE du Conseil du 25 juillet 1985 relative au rapprochement des dispositions législatives, réglementaires et administratives des États membres en matière de responsabilité du fait des produits défectueux*

III. POUR UN DÉVELOPPEMENT DE L'ÉCONOMIE DES DONNÉES MAIS UNE ATTENTION FORTE QUANT AUX LACUNES DANS LA MISE EN ŒUVRE

Vos rapporteurs soutiennent pleinement l'action de la Commission européenne pour l'établissement d'une liberté de circulation des données non personnelles. L'apport d'une telle proposition de règlement à la croissance économique du secteur n'est pas négligeable. L'essor de l'économie du numérique, tant sur le plan de l'innovation que celui de l'investissement, est lié à la restauration de la confiance des acteurs privés. La régulation de la circulation des données par un principe unique, harmonisé à l'échelle de l'Union européenne, mettrait fin à toute incertitude sur le plan juridique. C'est pourquoi vos rapporteurs encouragent la suppression de toute règle nationale injustifiée qui constituerait un obstacle potentiel à la libre localisation des données au sein du marché intérieur. L'adoption d'une régulation européenne est d'autant plus nécessaire qu'il convient d'éviter une éventuelle exclusion de l'Union européenne comme acteur essentiel dans ce domaine au niveau international. La localisation des données doit être une décision émanant des entreprises clientes des services numériques et non un choix imposé par le législateur comme le soutient l'AFNUM.

Vos rapporteurs tiennent à souligner le fait que l'utilisation d'un « *cloud* souverain » serait contre-intuitive, voire nuirait à la productivité et la sécurité des entreprises. En effet, les données sont des biens qui sont amenés à circuler en permanence et dont le déplacement peut difficilement être restreint à un espace géographique clos. Pour produire une valeur conséquente, les données doivent être accessibles au moins sur un marché de la taille de celui de l'Union européenne. C'est la seule façon de permettre aux entreprises de rester compétitives en diminuant leurs coûts d'infrastructure et en accédant à un marché d'une taille suffisante pour favoriser les économies d'échelle. Ceci est d'autant plus vrai compte tenu de la digitalisation d'un grand ensemble de secteurs économiques. De même, la sécurité des données n'est pas assurée de manière plus efficace si celles-ci sont localisées au sein d'un seul et même État. La dispersion des données dans différents serveurs pourrait au contraire favoriser leur sécurité, puisque toute forme de piratage serait d'autant plus difficile.

En outre, afin de protéger les utilisateurs, individu ou entreprise, vos rapporteurs encouragent la création d'un droit à la portabilité afin que les utilisateurs de services numériques contrôlent pleinement l'exploitation de leurs données. Différents acteurs auditionnés, à l'instar du CNNum, ont mis en avant le fait que la portabilité se faisait davantage entre les fournisseurs que de manière transfrontalière. Elles ont également émis la volonté de participer à un dialogue avec les autorités publiques pour établir des règles concrètes pour assurer la mise en œuvre de ce droit. De la même manière, la DG CONNECT encourage les États membres à rencontrer l'industrie dans le cadre des réflexions sur les nouvelles

législations à venir. Cette coconstruction des règles avec le secteur privé permettrait d'en assurer le caractère opérationnel, d'autant que l'application d'un tel règlement peut représenter un coût certain et mobiliser du temps dont les entreprises ont besoin pour développer leur activité en dehors de la gestion des données. Il est donc nécessaire d'informer les acteurs des bénéfices à long terme que peut apporter la mise en place de telles mesures.

Vos rapporteurs notent toutefois que les mesures proposées par la Commission européenne pour garantir aux autorités nationales l'accès aux données, doivent respecter entièrement la capacité des autorités publiques à garantir la sécurité des citoyens. Ainsi, il est nécessaire d'accompagner la libre circulation des données par un processus de coopération renforcée et effective entre les organes nationaux en charge dans chaque État membre. Or, les autorités françaises ont fait part de leur doute quant à la coopération interétatique. La procédure d'assistance n'est en effet pas détaillée dans la proposition, aucune modalité telle qu'un délai de réponse ou des sanctions en cas de non-coopération, n'est précisée. Dans une telle situation, la coopération ne pourra que difficilement être rendue obligatoire. De même, la question de l'absence d'harmonisation des procédures d'accès aux données dans les États membres a été soulevée par les représentants de Microsoft. Le règlement n'indique pas quelle procédure légale devra s'appliquer entre celle l'État membre où sont hébergées les données et celle de l'État membre demandant l'accès. Cette fragmentation des législations entraînera une coopération plus inefficace et juridiquement plus incertaine.

La sécurité dans l'usage des données passe aussi par la responsabilisation des fournisseurs de services. L'adoption des codes de conduite autorégulateurs, incluant une obligation de transparence entre autres, est ainsi pertinente. Pour vos rapporteurs, ce n'est donc pas tant la localisation des données qui constitue le principal problème, mais la capacité des autorités nationales et européennes à avoir toujours accès aux données lorsque l'intérêt général l'exige, de manière nécessaire et proportionnée.

Néanmoins, la proposition de la Commission européenne présente des lacunes potentiellement problématiques en vue de la mise en place d'une circulation effective des données. D'une part, il est nécessaire d'harmoniser les modalités de sécurité que doivent présenter les centres de stockage de données au niveau européen. En effet, si les données de tout citoyen européen peuvent être localisées dans n'importe quel État membre, cela implique un niveau de protection équivalent dans l'ensemble des États membres. Or, les normes régulant les centres de données ne sont pas harmonisées dans les législations nationales comme le rappellent les autorités françaises dans leur positionnement contre la proposition actuelle de règlement.

D'autre part, d'un point de vue juridique, les acteurs économiques auditionnés ont fait ressortir un manque de définition du champ d'application du règlement. La frontière entre le caractère personnel ou non d'une donnée est parfois mince et la proposition de règlement gagnerait à être plus précise.

Notamment, il s'agit de comprendre l'articulation exacte avec le RGPD. Certains types de données peuvent être l'objet d'interprétations variées, c'est le cas par exemple des données publiques anonymes. Elles peuvent tout aussi bien être exclues du champ d'application compte tenu de nécessités d'ordre public, ou être inclues dès lors qu'elles ne possèdent aucun biais permettant d'identifier l'individu dont elles proviennent. Les représentants de SAP ont insisté sur la difficulté de définir quelles données pouvaient être qualifiées de sensibles et donc être exclues du champ de ce règlement. L'exception de sécurité publique fait courir le risque d'une forme d'imprécision puisque les différents États membres ont chacun une conception propre de ce terme.

Une autre définition doit être approfondie : est concerné par la proposition tout fournisseur établi en Europe. Cette définition ne semble pas garantir l'application stricte des mesures du règlement à des entreprises extra-européennes proposant des services numériques dans l'Union européenne. Il convient donc de mettre au point des mécanismes pour assurer le respect uniforme des mesures par tout acteur exerçant sur le territoire européen. La CSNP a notamment alerté vos rapporteurs sur cette question, mettant en avant la difficulté de contrôler l'application du droit européen par les acteurs américains ou chinois par exemple.

Enfin, la Commission européenne n'a pas indiqué si cette nouvelle liberté au sein du marché intérieur pourrait faire partie des sujets de négociations de futurs accords de libre-échange. Vos rapporteurs souhaitent affirmer que l'utilisation et la protection des données européennes doivent être encadrées par le droit européen en vigueur. Dans le cas d'une extension de la liberté de circulation aux territoires extracontinentaux, il conviendra de garantir un contrôle strict du respect de ces règles. Ainsi, au vu de l'état actuel du droit, il faut exclure la possibilité de faire entre le champ des données dans le cadre d'un accord de libre-échange.

TROISIÈME PARTIE : LA CYBERSÉCURITÉ

I. LA PRISE DE CONSCIENCE D'UN BESOIN DE RENFORCEMENT DE LA SÉCURITÉ DANS LE DOMAINE DU NUMÉRIQUE

Le développement de l'usage des services numériques va de pair avec l'accroissement de l'impact que des failles sécuritaires peuvent avoir sur les utilisateurs. L'Union européenne soutient la nécessité de renforcer la sécurité en ligne afin de protéger l'ensemble de l'économie européenne, estimant que 80 % des entreprises européennes ont dû faire face à une cyberattaque en 2016[1]. Par ailleurs, l'interconnexion et l'interdépendance des réseaux européens entraînent une propagation plus large de ce genre d'attaques d'un point de vue géographique et sectoriel. Ce sont les raisons pour lesquelles la Commission souhaite mettre en place une politique renforcée en termes de cybersécurité, incarnée par le paquet « cybersécurité ».

A. L'ÉTABLISSEMENT D'OUTILS NÉCESSAIRES À LA GESTION DE CRISES POTENTIELLES

1. Un organe central pour coordonner les stratégies et apporter son expertise en matière de cybersécurité : l'ENISA

La volonté qui a présidé à la constitution d'une réponse commune européenne aux menaces en matière de cybersécurité a conduit à la mise en place d'une agence commune.

Le fonctionnement de l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA)

L'Agence européenne chargée de la sécurité des réseaux et de l'information (ENSIA), instituée en mars 2004 par le Règlement (CE) n° 460/2004, pour un mandat de cinq ans, est principalement chargée d'assurer le conseil et la coordination des mesures prises par la Commission et les pays de l'Union européenne en ce qui concerne la sécurité des réseaux et de l'information. Cette agence vise à renforcer la capacité de l'Union européenne, ainsi que des pays de l'Union européenne, en matière de prévention, de réaction et de gestion des problèmes liés à la sécurité des réseaux et de l'information. À cette fin, elle facilite et encourage la coopération entre les acteurs des secteurs publics et privé, afin d'établir un haut niveau de sécurité dans les pays de l'Union.

L'une des principales missions de l'agence réside dans la collecte d'informations afin d'analyser les risques sur la résilience des réseaux de communications, et sur la confidentialité ainsi que l'intégrité des communications. L'ENISA possède aussi un rôle de

[1] *Commission européenne. Discours sur l'État de l'Union prononcé par Jean-Claude Juncker le13 septembre 2017 devant le Parlement européen à Strasbourg.*

prévention pour sensibiliser les différents acteurs, publics et privés, du marché numérique à de meilleures pratiques. Elle a par ailleurs pour mission de coopérer avec les États membres dans le but de développer les outils nécessaires à la sécurité numérique au niveau européen, dans la prévention et la gestion des risques.

Basée à Héraklion en Grèce depuis le 1er septembre 2005, elle est constituée d'un conseil d'administration, d'un directeur exécutif et d'un groupe permanent représentant les parties prenantes composé de représentants des entreprises du secteur des technologies de l'information et de la communication, de consommateurs et d'experts universitaires. Ce groupe, permettant à l'ENSIA d'avoir accès aux informations les plus récentes, émet des conseils aux institutions européennes et aux États membres.

Le Parlement européen, la Commission européenne ou une autorité réglementaire nationale peuvent faire appel à l'ENISA afin que celle-ci leur apporte son soutien en matière de conseils ou d'assistance. Cette demande doit être adressée au directeur exécutif.

Suite à une communication de la Commission européenne en 2009[1] et à un renouvellement du mandat de l'agence en 2008[2], l'ENISA a été dotée de nouvelles prérogatives afin d'améliorer la résilience. En particulier, la protection des infrastructures d'information critiques est alors au centre du débat avec le début de la discussion de la directive SRI[3]. L'agence doit apporter son soutien à la mise en place d'une politique de protection des infrastructures numériques. Son rôle est toutefois cantonné aux limites du cadre de l'expertise et la puissance opérationnelle demeure du ressort exclusif des États membres.

Enfin, une coopération a été instaurée avec Europol pour renforcer la prévention et la détection des cybercrimes. Cette tâche lui a été attribuée en 2013 par voie de règlement et s'est accompagnée d'une extension de son mandat pour une durée de sept ans[4]. Depuis 2010, l'ENISA organise régulièrement des exercices de simulations d'incidents afin de renforcer la qualité des réponses émises par les États membres en cas de crise.

2. Les mécanismes européens de réponse permettant une forme de coordination en cas de crise

Différents mécanismes ont été institués au niveau européen afin de répondre de manière coordonnée à des crises liées ou non au numérique, en parallèle de la création de l'ENISA. Un certain nombre d'entre eux sont purement

---

[1] *Commission européenne. Communication « Protéger l'Europe des cyberattaques et des perturbations de grande envergure : améliorer l'état de préparation, la sécurité et la résilience », COM(2009)149, 30 mars 2009.*

[2] *Règlement (CE) 1007/2008 du Parlement européen et du Conseil du 24 septembre 2008 modifiant le règlement (CE) n° 460/2004 instituant l'Agence européenne chargée de la sécurité des réseaux et de l'information en ce qui concerne sa durée*

[3] *Directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union*

[4] *Règlement (EU) 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) n° 460/2004*

tournés vers le domaine pénal, à l'instar d'Europol, ou se concentrent sur des domaines diplomatiques, comme le mécanisme de réponse aux crises du Service européen pour l'action extérieure (SEAE), le CRM[1]. Le dispositif intégré pour une réaction au niveau politique dans les situations de crise (IPCR), quant à lui, permet de prendre des décisions politiques rapides et coordonnées à l'échelle de l'Union européenne en cas de crise majeure.

Néanmoins, un outil a été introduit afin d'encadrer la coordination des actions en cas de crise majeure et multisectorielle. Il s'agit d'ARGUS, créé en 2005, complété par un système d'alerte rapide du même nom. Bien que la gestion de crise relève majoritairement de la responsabilité des États membres, l'Union européenne a un rôle à jouer lorsque l'incident touche les domaines relevant de sa compétence, se déroule dans plusieurs pays à la fois ou afin d'assister un État. Chaque Direction Générale de la Commission européenne peut informer les autres d'un possible risque de crise multisectorielle et activer le processus de notification rapide d'alerte d'ARGUS.

Une première phase prévoit l'échange d'information sur une crise d'ampleur limitée. La seconde phase du dispositif, activée par le Président de la Commission européenne ou des membres de la Commission, enclenche la réunion du comité de coordination de crise (CCC), dirigé par le Président de la Commission ou le commissaire en charge. Le CCC est composé de membres de différentes Directions Générales et d'autres services des institutions de l'Union européenne pertinents pour régler la crise. Ces réunions permettent d'évaluer la situation et de décider d'utiliser des instruments dont la Commission européenne a la responsabilité.

Enfin, les institutions européennes étant régulièrement prises pour cible par les acteurs malveillants, un instrument a été établi sur le modèle des centres de réponse aux incidents de sécurité informatique (CSIRT) : le CERT-UE. Il agit en cas d'urgence au sein des organes européens. Il peut aussi participer à la coopération du réseau européen des CSIRT.

[1] *Commission européenne. Annexe de la recommandation de la Commission sur la réaction coordonnée aux incidents et crises de cybersécurité majeurs, C(2017) 6100, 13 septembre 2017.*

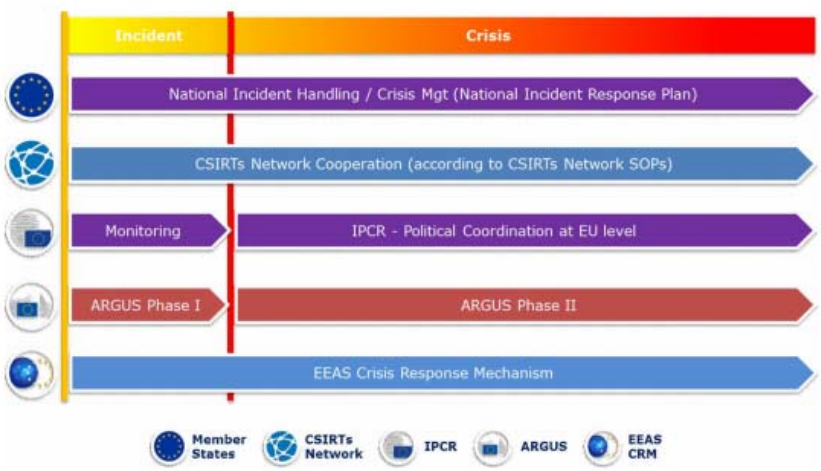

Figure 1 : les mécanismes de réaction à un incident au niveau de l'Union européenne, source : Commission européenne

Comme le montre le schéma ci-dessus, seuls les mécanismes nationaux, c'est-à-dire les institutions nationales en charge ou les CSIRT, sont activés tout au long de la crise. Cela permet de respecter la subsidiarité, les compétences de sécurité revenant aux États membres. Dès lors, aucun mécanisme de gestion de crise ne permet actuellement une coopération renforcée et obligatoire entre les États membres dans le domaine du numérique.

B. LES PRÉMICES D'UNE RÉGLEMENTATION EUROPÉENNE POUR HARMONISER LES COMPORTEMENTS NATIONAUX : LA DIRECTIVE SRI

Le premier acte législatif européen en matière de cybersécurité s'est intéressé aux secteurs économiques les plus sensibles. Certains secteurs essentiels au fonctionnement des économies nationales, tels que les banques et les infrastructures financières, étaient déjà encadrés par des règles sectorielles. La directive du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information[1] a toutefois véritablement renforcé l'harmonisation et la coopération en matière de gestion des risques.

1. Développer une culture de la gestion des risques chez des acteurs économiques fondamentaux

Cette directive s'adresse avant tout aux opérateurs de services essentiels (OSE) et aux fournisseurs de services numériques (FSN). Ces deux types d'entreprises exercent leurs activités dans les secteurs de l'économie les plus

[1] *Directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union*

vulnérables aux attaques car ils ont un rôle central dans la société ou sont les plus propices à être touchés puisque leurs produits ou services sont numériques. La directive ne cite que les secteurs généraux considérés comme particulièrement nécessaires au fonctionnement normal de la société[1], tels que l'énergie, les transports, les banques et les marchés financiers, ou encore la santé, l'eau et les infrastructures numériques. Il revient aux États membres d'identifier nominativement les entreprises, publiques ou privées, avant le 9 novembre 2018, soit six mois après la fin du délai de transposition de la directive. En ce qui concerne les fournisseurs de services numériques, il s'agit de moteurs de recherche, de services d'informatique en nuage ou de plateformes de commerce en ligne. Les réseaux sociaux et les micro-entreprises sont exclus du champ d'application de cette directive.

Ce sont donc ces deux catégories d'acteurs qui sont particulièrement concernées par la directive et qui devront mettre en place des outils et des mécanismes renforcés de sécurité. Ils pourront se fonder sur des règles nationales que les États membres sont libres d'établir avant le 9 mai 2018, soit la fin du délai de transposition de la directive. Par ailleurs, les entreprises concernées par la directive auront l'obligation de notifier à l'autorité nationale compétente tout incident majeur afin de constituer un fond de données exploitables pour mettre en place des outils de résilience nationale. Par cette directive, la Commission européenne cherche à sensibiliser les entreprises aux risques liés à la cybersécurité et à instaurer une gestion des incidents efficace.

2. Améliorer la capacité et la coopération des États membres

La mise en place d'un réseau de CSIRT est l'outil central pour élever le niveau de cybersécurité européen. Ainsi, les États membres doivent désigner un CSIRT et un centre de réponses aux urgences informatiques (CERT). Les deux entités peuvent être regroupées au sein d'une même autorité nationale. Leur rôle est d'alerter, de suivre et d'analyser les incidents pour développer des mécanismes de réponse rapide. Un point de contact unique a également été développé, à destination des entreprises.

Le cadre réglementaire européen incite donc à la coopération volontaire entre les États membres, via un « groupe de coopération », constitué de représentants de la Commission européenne, des États membres et de l'ENISA et un réseau européen des CSIRT. Ce réseau, structuré par une stratégie commune, doit partager les informations nécessaires pour renforcer la prévention. Les autorités nationales ont donc un devoir d'entraide lors d'incidents transfrontaliers. Il n'existe cependant pas de cadre de coopération en cas de crise majeure

[1] *Article 4 et annexe II de la directive (UE) 2016/1148*

dépassant les secteurs couverts par la directive, comme l'a souligné le Conseil dans ses conclusions à propos de la cyber-résilience[1].

Enfin, la capacité des États membres à faire face à d'éventuelles attaques cyber devra être exposée à la Commission européenne dans un « plan d'évaluation des risques » inclus dans un plan national de coopération en matière de SRI, au plus tard un an et demi après l'adoption de la directive, soit à la fin de l'année 2017. Celui-ci doit être présenté par les États membres dans le cadre de leur stratégie nationale pour développer des moyens de sécurité novateurs[2].

[1] *Conseil de l'Union européenne. Conclusions du Conseil intitulées « Renforcer le système européen de cyber-résilience et promouvoir la compétitivité et l'innovation dans le secteur européen de la cybersécurité », document n° 14540/16 du 15 novembre 2016*

[2] *Article 5 de la directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union*

II. LE PAQUET « CYBERSÉCURITÉ » : LA CRÉATION D'UNE VÉRITABLE POLITIQUE EUROPÉENNE UNIFIÉE

Lors de son dernier discours sur l'État de l'Union, le 13 septembre 2017, le Président de la Commission européenne, Jean-Claude Juncker, a mis en avant la pertinence d'une politique européenne de cybersécurité : « Les cyberattaques sont parfois plus dangereuses pour la stabilité des démocraties et des économies que les fusils et les chars. […] Les cyberattaques ne connaissent pas de frontières ; elles n'épargnent personne. ». C'est dans le cadre de cette impulsion politique que la Commission européenne a présenté son paquet de propositions en matière de cybersécurité le 19 septembre 2017.

Les différents outils disponibles jusqu'alors restent en effet limités à certains secteurs et à des cas de figure spécifiques. Le paquet « cybersécurité » tend à protéger davantage le marché intérieur, en simplifiant les mécanismes de sécurité numérique. En effet, la fragmentation des approches et des ressources nationales ou européennes à l'égard de la cybersécurité mais aussi le manque de sensibilisation des citoyens et des entreprises à ces menaces sont des obstacles à l'établissement d'une sécurité pourtant nécessaire au sein du marché intérieur.

A. UN STATUT PÉRENNE DE L'ENISA VIA L'ÉTABLISSEMENT DE L'AGENCE DE LA CYBERSÉCURITÉ DE L'UNION EUROPÉENNE

Le « paquet » contient le projet de réforme du mandat et du statut de l'actuelle ENISA afin de mettre en œuvre de manière plus efficace la directive SRI et de préparer les outils nécessaires aux États membres et à l'Union européenne pour faire face aux crises.

Les nouvelles attributions de l'agence seraient articulées autour de cinq points, à la fois en reprenant les compétences actuelles de l'ENISA, tout en introduisant des capacités inédites et avancées :

- Les activités de Conseil auprès des législateurs européens et nationaux dans le domaine général de la cybersécurité mais aussi particulièrement pour la mise en œuvre de la directive SRI. ;

- La coopération opérationnelle est également renforcée. Ainsi, l'agence n'est plus limitée aux simples compétences d'expertise et de recommandation. Elle peut être amenée à coopérer avec les CSIRT et porter assistance directement à un État membre, à la demande de ce dernier ;

- L'agence doit aussi profiter de son expertise et de son expérience acquise durant la dernière décennie dans un but d'information et de prévention auprès des institutions publiques et des acteurs

privés. Elle collecte, analyse et rend disponibles des informations et des données émanant des différentes notifications d'incidents ;

- Enfin, ainsi que l'établit l'article 44 de la proposition de règlement, l'ENISA bénéficierait d'une option pour la formation d'un schéma de certification européen de cybersécurité, en se fondant tant sur son expertise propre que sur celles des autorités de certifications nationales.

Afin de mener à bien ces nouvelles missions, l'ENISA devrait voir ses capacités renforcées, via une augmentation de personnel (de quatre-vingts à cent vingt-cinq employés) et de son budget, qui passerait de 11 millions à 23 millions d'euros.

B. LA CRÉATION D'UN SCHÉMA DE CERTIFICATION POUR HARMONISER LES EXIGENCES SÉCURITAIRES DES PRODUITS ET SERVICES DES TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION (TIC)

Le schéma de certification européen de cybersécurité devrait donc être élaboré par l'ENISA avant d'être validé officiellement par la Commission européenne. Cette démarche a pour objectif d'éviter une fragmentation nationale du système de certification qui pourrait mener à des niveaux de sécurité différents d'un État membre à l'autre. Cela pourrait entraîner une rivalité réglementaire potentiellement néfaste à la compétitivité des pays les plus exigeants, à la sécurité générale et au développement du marché intérieur.

Une certification européenne est donc nécessaire pour garantir la confiance des utilisateurs et développer le marché unique du numérique. En particulier, la reconnaissance par tous les États membres d'un système de certification unique facilitera le commerce et la prestation de services transfrontaliers ainsi qu'une meilleure compréhension des utilisateurs quant à la nécessité d'un niveau de sécurité adapté. Une fois établie, l'application de cette certification sera coordonnée par l'ENISA. Les certifications seront toutefois délivrées par les autorités nationales compétentes, désignées par les États Membres. Elle consistera en une série de règles, standards, procédures et normes techniques auxquels devront satisfaire les produits et les services TIC. Il est à noter que le schéma de certification ne sera pas requis pour tous les produits et services mis en vente sur le marché. Sauf les domaines potentiellement identifiés par le droit européen, seules les entreprises volontaires pourront faire certifier leurs produits et services, afin de leur apporter une valeur ajoutée.

De manière plus concrète, la certification devra comprendre trois niveaux de sécurité à satisfaire en fonction du type de produits ou de services. Les trois niveaux de certification – élémentaire, substantiel et élevé – répondront à des objectifs différents. Certains produits numériques requièrent, en effet, par leur nature et leur utilisation un niveau de garantie plus élevé que d'autres. De même,

des niveaux différenciés permettent de ne pas exclure du champ d'application des produits pour lesquels un niveau de sécurité trop élevé entraînerait des coûts de conformité démesurés, en particulier pour les PME.

Cette idée de certification en matière de cybersécurité n'est par ailleurs pas nouvelle. Des schémas de certification existent déjà dans certains États membres, tels que la France mais aussi l'Allemagne, les Pays-Bas ou encore le Royaume-Uni. Par ailleurs, une initiative incluant douze États membres et la Norvège a abouti à une reconnaissance mutuelle de ces certificats. Il s'agit du système SOG-IS MRA, en place depuis 1999. Outre la reconnaissance mutuelle des certifications nationales, ce système promeut l'élaboration de standards communs uniformisés.

La certification française, la Certification de Sécurité de Premier Niveau (CSPN), mise en place par l'Agence nationale de la sécurité des systèmes d'information (ANSSI), jouit d'une réputation positive au sein de l'Union européenne. La certification est organisée autour de différentes catégories de produits exigeant des normes et des évaluations variées.

C. DES OUTILS POUR CONSOLIDER LA LUTTE CONTRE LES INCIDENTS

Mis à part la proposition de règlement, le paquet « cybersécurité » contient différentes propositions de la Commission européenne afin de promouvoir la recherche et le développement de nouveaux outils.

Dans sa recommandation à propos d'une réaction coordonnée aux incidents et aux crises de cybersécurité majeures[1], la Commission européenne souhaite créer un cadre permettant de renforcer la coopération, en instaurant notamment des procédures opératoires standards. De la même manière, elle propose de statuer plus concrètement sur la coopération entre les États membres et l'Union européenne en adoptant des mesures pratiques pour intégrer les organes et les procédures nationaux dans un mécanisme européen complet. La structure de ce cadre de coopération devrait être régulièrement revue par l'ENISA et les États membres afin de tirer les enseignements des expériences issus de chaque incident. Ce mécanisme pourra être facilité par l'adoption de rapports de situation ayant un modèle commun afin d'analyser au mieux les causes et les incidents de chaque crise.

Le développement d'un outil complet et efficace en matière de cybersécurité doit aussi être soutenu par une adaptation des compétences professionnelles. Le manque de personnes qualifiées pour répondre aux crises est un constat émanant tant des institutions nationales et européennes que des acteurs privés, notamment ceux faisant partie des personnes auditionnées. L'acquisition de connaissances approfondies sur le sujet est nécessaire afin de permettre la

[1] *Commission européenne. Recommandation sur réaction coordonnée aux incidents et aux crises de cybersécurité majeures du 13 septembre 2017, C(2017) 6100*

recherche et le développement mais aussi la pédagogie et la prévention auprès des citoyens et des entreprises européens. À ces fins, un Centre européen de recherche et de compétences en matière de cybersécurité sera institué au cours de l'année 2018. Il secondera les États membres dans l'augmentation de leurs capacités de résilience mais il aidera aussi à mettre au point les technologies nécessaires pour faire face aux risques. De la même manière, une plateforme de formation et d'enseignement en cybersécurité devrait combler le déficit de compétences professionnelles. Il faut développer un marché de professionnels experts en assistance des entreprises en cas de crise. En effet, les nouveaux risques existants sont peu compris et de nature nouvelle, voire toujours mouvante. Les entreprises ainsi que les administrations publiques ne peuvent pas être efficaces en employant des mécanismes de protection internes puisque ceux-ci sont très coûteux et requièrent des compétences spécifiques que les entreprises ne possèdent pas dans la majorité des cas.

Enfin, la Commission européenne propose la création d'un fonds d'intervention sur le modèle de l'actuel mécanisme de protection civile en cas de catastrophe naturelle. Il s'agirait d'inciter au respect des bonnes pratiques par les États membres en contrepartie d'une aide financière en cas d'urgence.

III. UNE AVANCÉE NOTABLE POUR LA SÉCURITÉ NUMÉRIQUE EUROPÉENNE MALGRÉ UNE COORDINATION A MINIMA

Vos rapporteurs saluent la volonté de la Commission européenne d'instaurer une politique de cybersécurité concrète à l'échelle communautaire. Néanmoins, ils retiennent le manque d'ambition de la proposition de règlement que ce soit par rapport à la certification des produits et des services numériques ou en ce qui concerne le rôle des autorités nationales en charge de la sécurité numérique.

Une certification européenne en la matière est nécessaire pour maintenir la confiance des utilisateurs dans les produits et les services connectés et ainsi développer ce marché économique. Vos rapporteurs estiment qu'une certification avec différents niveaux d'assurance est requise pour s'adapter aux types variés de produits et services. Particulièrement, ils considèrent qu'une structure en trois niveaux serait optimale pour avoir un équilibre entre une adaptation aux différentes entreprises sur le marché et une lecture assez claire des gradients de la certification. En effet, un nombre trop faible de niveaux aboutirait à une partition trop duale, cela pourrait entraîner une disproportion pour la protection de certains produits comme l'a indiqué M. Loesekrug-Pietri. À l'inverse, une certification avec une trop grande variété de catégories impliquerait un système trop instable et potentiellement trop coûteux. Afin de préserver l'innovation et l'activité des petites entreprises, qu'elles soient nouvelles ou traditionnelles, la certification doit rester sur une base volontaire et avoir des exigences cohérentes. De même, pour garantir la durabilité du système de certification, les normes requises ne doivent pas devenir obsolètes trop rapidement du fait de l'avancée technologique.

La faiblesse du système de certification proposé par la Commission européenne tient aussi au risque d'une harmonisation « par le bas » des normes européennes. L'ANSSI, l'autorité responsable en France pour la certification, possède déjà un cadre de certification reconnu et pertinent. Il serait dès lors préférable de se fonder sur l'expertise des autorités ayant déjà reçu des résultats concluants en matière de politique de sécurité. L'ANSSI précise que l'évolution vers une certification européenne est pertinente par rapport à la forte interconnexion des systèmes européens. Mais l'ENISA, dont les moyens demeurent encore limités, ne doit pas être le seul acteur dans le développement de ce mécanisme. Les agences nationales conservent toute leur pertinence, sans quoi le risque de cybermenaces pourrait augmenter d'autant.

Il est donc plus judicieux de laisser aux autorités nationales la charge des certifications et des actions en cas d'incident. Les États membres doivent rester garants de la protection des citoyens. C'est pourquoi le nouveau mandat de l'agence européenne ne doit pas lui affecter de nouvelles prérogatives qui bloqueraient l'action des autorités nationales. Vos rapporteurs estiment que

l'ENISA doit garder un rôle de coordination à l'échelle européenne et se reposer sur les agents nationaux pour agir concrètement. Cette coordination devrait permettre une montée en charge des agences nationales encore trop peu dotées dans certains États membres et leur faire atteindre un niveau d'exigence en harmonie avec celui des États membres plus avancés. Une défaillance dans le système de sécurité d'un État membre aurait, en effet, un impact sur l'ensemble des réseaux européens et donc sur la sécurité de tous les États membres.

Vos rapporteurs déplorent également le manque de maturité des entreprises privées face aux enjeux de cybersécurité. La prise de conscience de ces acteurs quant aux conséquences d'un incident informatique est tardive dans la plupart des cas et a le plus souvent lieu seulement après avoir été victime d'une attaque. Les autorités nationales et européennes doivent donc accentuer l'information aux citoyens et aux entreprises. Cela permettra de les sensibiliser au besoin d'investir dans des équipements de protection, même si les bénéfices tirés de ce financement ne sont pas directement visibles. La sécurité informatique représente certes une hausse des coûts de 5 % à 10 % pour les entreprises d'après l'ANSSI, mais les exigences relatives à la cybersécurité doivent devenir une évidence. Ces investissements dans des produits innovants soutiendraient par ailleurs la recherche et le développement d'entreprises fournissant des outils de sécurité.

QUATRIÈME PARTIE : POUR UNE FISCALITÉ DU NUMÉRIQUE JUSTE ET EFFICACE

Vos rapporteurs ont souhaité traiter d'un sujet qui n'est pas directement lié à la construction d'un marché unique du numérique, telle que la Stratégie pour un Marché Unique du Numérique l'entendait initialement. Mais la construction d'un système fiscal commun qui puisse assurer une concurrence équitable pour l'ensemble des acteurs dans le secteur du numérique constitue désormais un objectif majeur à l'échelle européenne.

I. L'INITIATIVE FRANÇAISE VISE, À JUSTE TITRE, À LUTTER CONTRE LES PRATIQUES D'ÉROSION DES BASES FISCALES DANS LE DOMAINE DU NUMÉRIQUE

A. LA PROPOSITION D'UNE TAXE DE PÉRÉQUATION S'INSCRIT DANS UN VASTE CHAMP DE RÉFLEXIONS INITIÉES DEPUIS PLUSIEURS ANNÉES

Il s'agit en premier lieu, bien évidemment, d'assurer la soutenabilité des finances publiques, comme le montrent les travaux menés par l'OCDE (Organisation de Coopération et de Développement Économiques) depuis 2013 sur l'érosion de la base fiscale et le transfert des bénéfices. Cette soutenabilité s'entend d'autant mieux que les entreprises du secteur numérique, malgré leurs grandes malléabilité et mobilité, s'appuient sur des infrastructures et sur un haut degré d'éducation, financés par les deniers publics. L'action I du Plan d'action de l'OCDE sur l'érosion de la base d'imposition et le transfert de bénéfices s'est en effet consacrée aux « défis fiscaux posés par l'économie numérique ».

L'idée d'une taxe d'égalisation n'est pas une initiative française isolée, puisqu'elle a pu être mise en place dans d'autres ensembles d'une taille comparable à celle du marché intérieur de l'Union européenne. C'est notamment le cas en Inde. Plus largement, l'initiative française s'appuie sur le projet à long terme d'évolution de l'impôt sur les sociétés. C'est pourquoi elle a reçu le soutien d'environ vingt États membres après sa présentation en septembre 2017. Cette taxe, dite également « de péréquation sur le chiffre d'affaires des entreprises numériques », se traduirait, selon l'appréciation de la Commission européenne, par une taxe sur l'ensemble des revenus non taxés, ou taxés de manière insuffisante, générés par toutes les activités économiques via internet. Le champ d'application de cette taxe comprendrait les activités entre entreprises, mais aussi,

entre entreprises et consommateurs. Elle serait imputable sur l'impôt sur les sociétés ou mise en œuvre comme une taxe distincte [(1)].

Le Conseil européen, en prenant en compte l'initiative française mais aussi la communication de la Commission, a encouragé le Conseil, lors de la réunion du 19 octobre 2017, à examiner rapidement cette communication, afin de faire en sorte que toutes les entreprises paient une part adéquate de leurs impôts et que soient assurées des conditions de concurrence équitables.

B. LA LUTTE CONTRE L'ÉROSION DE LA BASE FISCALE SUPPOSÉE DE PRENDRE EN COMPTE LES CARACTÉRISTIQUES PROPRES À L'ÉCONOMIE NUMÉRIQUE

Il convient de rattacher la base taxable à une implantation territoriale, de la même manière que ce qui se fait pour les sociétés s'appuyant sur des infrastructures physiques. La détermination de l'assiette des entreprises du secteur pose un problème en la matière, puisque celles-ci peuvent exercer une activité économique dans un État membre sans y posséder une immobilisation. La détermination de l'assiette doit donc évoluer pour refléter la valeur réelle des bénéfices réalisés par les entreprises digitales. Les caractéristiques de l'économie numérique comprennent notamment la mobilité des actifs incorporels des utilisateurs et des fonctions de l'entreprise ; le recours à une utilisation massive de données, issu de l'augmentation des capacités de stockage et de traitement algorithmique des données ; des effets de réseau, par lesquels les décisions prises par certains utilisateurs ont un impact direct sur les avantages dont peuvent bénéficier les autres utilisateurs ; le développement de modèles d'affaires multifaces, par le biais de plateformes au sein desquelles les décisions de chaque groupe affectent les résultats obtenus par l'autre groupe et bien sûr la volatilité due à l'abaissement des obstacles à l'entrée sur les marchés et à la rapidité d'évolution de la technologie, ainsi qu'à la vitesse avec laquelle des clients peuvent choisir d'abandonner des produits et des services déjà anciens pour en adopter de plus récents.

C'est dans cette mesure que l'économie numérique est plus susceptible que l'économie dite traditionnelle de profiter des failles dans les systèmes fiscaux nationaux. L'importance des actifs incorporels dans le contexte de l'économie numérique, ajoutée à la mobilité de ces actifs, offrent, dans le cadre des règles fiscales existantes, de larges possibilités d'érosion des bases fiscales et de transfert des bénéfices, notamment pour ce qui est des impôts directs. La fragmentation des activités physiques et la possibilité de développer une valeur ajoutée dans un État sans y installer d'infrastructure peut « miter » également l'assiette sur laquelle s'exerce l'impôt sur les sociétés. L'érosion de la base d'imposition survient en effet des pratiques qui séparent artificiellement le bénéfice imposable des activités qui le génèrent. Ces pratiques faussent également la concurrence entre les

(1) Communication de la Commission européenne « Un système d'imposition juste et efficace au sein de l'Union européenne pour le marché unique numérique » du 21 septembre 2017.

entreprises qui exercent leurs activités à l'échelle nationale, voire les multinationales qui respectent simplement l'intégrité des bases fiscales des États dans lesquels elles exercent leur activité.

Or, outre le fait que la digitalisation innerve désormais des pans de plus en plus larges des économies et des sociétés européennes, près du tiers de la production industrielle européenne est concernée par les technologies numériques. De la même manière, si en 2006, seule une entreprise digitale entrait dans la liste des vingt plus grosses capitalisations boursières, elles sont désormais neuf et comptent pour 54 % de la valeur boursière des vingt premières entreprises du classement. Enfin, des modèles particulièrement difficiles à prendre en compte dans les schémas actuels d'impôt sur les sociétés, comme les plateformes fondées sur des actifs extrêmement légers, doivent croître selon les prévisions d'environ 35 % par an dans les dix prochaines années. En moyenne, les modèles d'affaire numériques nationaux sont soumis à un taux d'imposition effectif de 8,5 % seulement, soit un taux deux fois moins élevé que celui appliqué aux modèles d'affaire traditionnels [(1)].

Dès lors, le principe qui a toujours sous-tendu l'application de l'impôt sur les bénéfices, à savoir le fait que celui-ci soit imposé là où la valeur est créée, n'est plus applicable. La Commission européenne, dans sa communication, relève donc deux défis majeurs pour adapter la fiscalité au « monde numérisé » :

« - Déterminer le lieu d'imposition (où taxer ?) – comment établir et protéger les droits d'imposition dans un pays où les entreprises peuvent fournir des services par voie numérique avec une présence physique faible ou inexistante, même si elles ont une présence commerciale ; et

- Définir l'objet de l'imposition (que taxer ?) – comment imputer les bénéfices dans de nouveaux modèles d'affaire numérisés fondés sur des actifs incorporels, des données et des connaissances. »

II. LES RÉFLEXIONS EN COURS DOIVENT PERMETTRE D'ASSURER LA CONTRIBUTION ÉQUITABLE DES SOCIÉTÉS NUMÉRIQUES AUX COMPTES PUBLICS

A. INSTAURER DE GRANDS PRINCIPES SUSCEPTIBLES DE RÉSISTER AUX RAPIDES ÉVOLUTIONS TECHNOLOGIQUES

Pour répondre à ces défis, il convient avant tout, selon vos rapporteurs, de s'entendre sur de grands principes. Le rythme des évolutions technologiques suppose en effet la définition d'un cadre large et moderne, seul à même de demeurer malgré les évolutions technologiques à venir. La Commission européenne en identifie quatre :

(1) Digital Tax Index, PWC et ZEW, 2017.

- l'équité, soit la possibilité de veiller à ce que les bénéfices des sociétés soient imposés là où la valeur est créée. C'est une nécessité pour maintenir des conditions de concurrence équitables et un système résilient ;

- la compétitivité, qui suppose de créer des conditions fiscales appropriées pour l'essor des entreprises numériques au sein du marché unique. Il convient donc d'éviter les entraves fiscales nationales, qui tiennent notamment à la fragmentation des systèmes fiscaux au sein de l'Union ;

- l'intégrité du marché unique, dès lors que de nouvelles distorsions et de nouveaux obstacles fiscaux entraveraient la croissance des entreprises ;

- la durabilité, soit la mise en place d'un système d'imposition des sociétés à l'épreuve du temps, durable et à même de préserver l'intégrité des bases fiscales nationales.

B. DÉTERMINER UNE ASSIETTE PERTINENTE SUR LAQUELLE APPLIQUER UNE TAXE D'ÉGALISATION

Les réflexions portent, à l'heure actuelle, sur les formes de rattachement de l'impôt sur les sociétés à la « présence numérique » dans chaque État membre. Dans le cadre des réflexions européennes a émergé l'idée de fonder l'assiette sur les données, mais la valeur de celles-ci est particulièrement difficile à évaluer. Les données sont en effet particulièrement hétérogènes : si un octet constitue une échelle déterminée, ce dernier peut porter des informations tout à fait différentes, du transfert de simples photos, par exemple, à celui de données bancaires. La fondation d'une assiette sur la seule estimation des données échangées ne permettrait pas de refléter la valeur réelle de l'activité des entreprises numériques. C'est ce qu'ont expliqué notamment les représentants de Google, pour qui une telle taxe sur les données ne pèserait pas uniquement sur les acteurs désormais traditionnels de l'activité numérique, mais aussi sur toutes les autres entreprises, dans le secteur automobile notamment, qui utilisent des données. M. Grégoire Tirot, Directeur de cabinet du Secrétaire d'État au numérique, a ainsi expliqué que le principe de territorialité de la résidence fiscale, telle qu'elle s'attache à la détermination traditionnelle de l'assiette de l'impôt sur les sociétés, ne fonctionne pas pour ce qui est des entreprises numériques.

Dès lors, vos rapporteurs soutiennent l'initiative française en ce qu'elle cherche à fonder l'assiette fiscale sur le chiffre d'affaires des entreprises digitales, tout en prenant en compte les spécificités de l'activité de ces sociétés. En particulier, le calcul de l'assiette pourrait s'appuyer également sur le nombre d'internautes par État membre, pour ce qui est de la répartition de l'impôt sur les sociétés, après consolidation. Par ailleurs, la détermination de la valeur taxable doit prendre en compte l'activité dans chaque État membre, par le biais de la collecte de données, en fonction des informations récoltées, mais aussi par la présence de points de vente plus traditionnels. En parallèle, cette valeur doit être calculée sans oublier les dépenses des entreprises numériques pour attirer les

internautes, par le biais, entre autres, de la publicité ciblée en ligne. On s'approche par ce biais de ce que l'OCDE considère comme une « présence économique significative » qui justifie une nouvelle forme d'imposition. Cette présence serait déterminée à partir de facteurs susceptibles de démontrer une interaction volontaire, inscrite dans la durée, avec l'économie de l'État, par le biais de technologies spécifiques ou d'outils automatisés, ainsi qu'un facteur de recettes. Tandis que le premier recoupe la nécessité de posséder un nom de domaine local, un nombre significatif d'utilisateurs mensuels actifs ou encore la conclusion de contrats en ligne, le second impliquerait notamment les revenus générés par l'usage des données d'utilisateurs dans un pays. La Commission européenne partage ce constat, puisque l'on trouve dans la communication du 21 septembre le point suivant : « les règles relatives à l'établissement stable servent à déterminer le seuil d'activité à réaliser dans un pays pour qu'une entreprise puisse être taxée dans ce pays et elles reposent essentiellement sur la présence physique. Cependant, grâce aux technologies numériques, les entreprises sont désormais en mesure d'avoir une présence économique significative dans une juridiction du marché intérieur sans nécessairement avoir une présence physique substantielle. D'autres indicateurs d'une présence économique significative sont dès lors requis afin d'établir et de protéger les droits d'imposition en ce qui concerne les nouveaux modèles d'affaire numérisés. »

La position des autorités françaises à l'heure actuelle en faveur d'une taxe d'égalisation tient de la solution de court terme, à défaut de mécanisme défini à l'échelle des pays de l'OCDE, auxquels s'associent, pendant ces travaux, les grands pays émergents ainsi que de nombreux pays en développement. Il s'agirait d'une imposition sur les chiffres d'affaires et non les bénéfices eux-mêmes. Cette modification de l'assiette permettrait d'éviter immédiatement, même si sans doute de manière encore un peu grossière, les mécanismes de transfert des bénéfices. La question demeure toutefois de savoir dans quelle mesure la présence d'une entreprise numérique pourra être déterminée afin qu'elle puisse contribuer de manière juste et équitable au budget public de l'État dans lequel la valeur est créée. Cette taxe d'égalisation ne fonctionnerait que de manière approximative par rapport à ce qui pourra être issu notamment des réflexions de l'OCDE au printemps 2018, mais cela permettrait déjà d'agir rapidement, alors même que la plasticité des entreprises du numérique implique une législation agile.

L'Union européenne constitue la bonne échelle d'intervention pour cette taxe. Il est en effet illusoire pour la France d'agir seule dans ce domaine, dès lors que 125 conventions fiscales la lient à d'autres pays, à commencer par ses principaux partenaires européens. Dès lors, une telle modification de l'impôt sur les sociétés ne peut intervenir qu'à l'échelle européenne, et ce d'autant plus compte tenu des lourdes contraintes que comporte le marché intérieur. Une initiative uniquement française serait porteuse de risques de délocalisation d'entreprises très mobiles, sans compter le poids excessif et discriminant qu'elle ferait porter sur les nombreuses jeunes pousses de l'écosystème numérique français. Il s'agit de l'un des dangers majeurs identifiés par le Conseil national du

numérique [1] dans ses travaux sur cette matière. Le Conseil national du numérique :

- « estime que la mise en place de nouvelles taxes nationales spécifiques au numérique ne contribuera aucunement à l'objectif de rééquilibrage fiscal entre les acteurs ayant un siège ou un établissement stable en France et les entreprises adoptant des comportements d'optimisation fiscale déloyale ;

- recommande, sans préjuger de l'évolution continue des dispositifs sectoriels, que les décisions en la matière tiennent compte du fait que les choix de la France seront autant de signaux envoyés aux partenaires de la négociation internationale. Sans exclure les adaptations, notamment jurisprudentielles, cela implique à tout le moins la prudence en matière d'établissement de nouvelles taxes sectorielles tant que cette négociation ne sera pas avancée ;

- déconseille la mise en œuvre immédiate et unilatérale des différentes propositions versées dans le débat public. »

De plus, les négociations actuelles sur les directives établissant une assiette commune consolidée pour l'impôt sur les sociétés (ACCIS) [2] pourraient aboutir à des propositions législatives dans le courant de l'année 2018. Or, le travail sur l'inclusion de la présence économique des entreprises numériques, en dehors de leur établissement physique, pourrait s'intégrer avantageusement aux réflexions sur la consolidation des bénéfices des services numériques entre États membres. Plus globalement, la mise en place d'une ACCIS permettrait de limiter drastiquement les mécanismes de transfert de bénéfices au sein de l'Union européenne, même si la clé de consolidation de cette assiette à l'échelle européenne demande à être encore précisée. Par ailleurs, cette assiette commune ne pourrait régler les problèmes posés par une implantation physique extra-européenne, si celle-ci demeure le critère d'éligibilité à l'impôt sur les sociétés.

Enfin, l'Union européenne travaille actuellement sur cette idée à l'échelle internationale, au sein de l'OCDE qui doit remettre son rapport consacré à cette question au G20 au cours du printemps 2018. La mise en place d'un système unifié à l'échelle européenne permettrait de définir un standard adaptable par la suite à l'échelle des principales puissances numériques mondiales. C'est en ce sens que vos rapporteurs soutiennent à la fois les efforts de la Commission européenne, de la présidence estonienne et des autorités françaises pour aboutir rapidement, et si possible dès début 2018, à une approche commune. Vos rapporteurs souhaitent par ailleurs que la Commission européenne, qui travaille actuellement sur une proposition législative en faveur d'une fiscalité équitable sur les acteurs numériques, puisse la présenter au même moment que la remise du

---

[1] *Avis n° 2013-3 du Conseil national du numérique, septembre 2013.*

(2) Proposition de directive du Conseil concernant une assiette commune pour l'impôt sur les sociétés du 25 octobre 2016 et proposition de directive du Conseil concernant une assiette commune consolidée pour l'impôt sur les sociétés (ACCIS) du 25 octobre 2016.

rapport de l'OCDE. Cette concomitance permettrait aux États membres et à l'Union européenne de parler d'une seule voix dans les enceintes internationales. De plus, le système fiscal européen fonctionnera globalement toujours mieux à partir du moment où celui-ci sera en phase avec les conclusions d'une enceinte multilatérale comme celle de l'OCDE. C'est à cette condition, selon vos rapporteurs, que l'Union européenne sera en mesure d'assurer le développement économique d'entreprises économiques européennes sur des bases équitables.

En termes plus techniques, vos rapporteurs estiment que si le principe d'une taxation sur le chiffre d'affaires aurait le mérite de la simplicité, il convient de rester ouvert à toute autre détermination d'une assiette taxable, dès lors qu'elle respecte les principes cardinaux d'effectivité, de transparence et d'équité.

Il convient, dans le même temps de développer les moyens d'assistance au recouvrement tels qu'ils existent déjà dans le cadre de l'OCDE.

C. ÉLARGIR LA RÉFLEXION AU-DELÀ DE LA SEULE QUESTION DU SECTEUR NUMÉRIQUE

Ce processus ne doit toutefois pas aboutir à isoler l'économie numérique du reste des activités économiques. Comme l'OCDE le relève, l'économie numérique s'assimilant de plus en plus à l'économie proprement dite, il serait difficile, pour ne pas dire impossible, de la distinguer du reste de l'économie dans une optique fiscale. Les nouveaux modèles partagés tant par les entreprises traditionnelles que par les nouveaux acteurs sont le commerce électronique, les services de paiement en ligne, les sites de vente d'applications en ligne, l'informatique en nuage, les plateformes participatives en réseau... Dès lors, « la possibilité de gérer leurs activités de façon centralisée tout en conservant une grande liberté dans le choix de l'implantation de leurs fonctions économiques a rendu les entreprises mieux à même de distribuer ces fonctions et leurs actifs entre différents pays. La mondialisation des activités au sein d'organisations de grande envergure n'est certes pas un phénomène nouveau, mais le développement de l'économie numérique conjugué à l'importance croissante de la composante des services, ainsi qu'à la réduction des coûts commerciaux ayant résulté de la libéralisation des échanges et de l'investissement et des réformes des réglementations, ont permis d'aplanir les obstacles logistiques et d'accélérer le mouvement. » [(1)] . Vos rapporteurs partagent l'idée exprimée par les représentants des acteurs du numérique selon laquelle les entreprises digitales ne sont pas les seules à mettre en place des schémas d'optimisation fiscale, et ce d'autant plus que la numérisation des entreprises traditionnelles est croissante.

De la même manière, il ne semble pas juste d'appliquer une retenue à la source pour la taxe d'égalisation, ainsi que l'Inde la pratique. Outre le fait que

---

(1) OCDE (2017), Relever les défis fiscaux posés par l'économie numérique, Action 1 - Rapport final 2015, Projet OCDE/G20 sur l'érosion de la base d'imposition et le transfert de bénéfices, Éditions OCDE, Paris. http://dx.doi.org/10.1787/9789264252141-fr.

l'application de la retenue à la source dans ce contexte serait porteuse d'iniquité, dès lors que les consommateurs supporteraient la véritable charge fiscale, elle pourrait s'avérer globalement inefficace.

Vos rapporteurs se félicitent donc en premier lieu de la prise en compte réelle du problème d'érosion de la base fiscale et de transfert des bénéfices par les entreprises du numérique. Ils insistent toutefois sur le fait que, aussi dommageable que l'absence de solution à l'échelle de l'OCDE puisse être pour l'effectivité de la lutte contre les pratiques d'optimisation fiscale, celle-ci ne doit pas empêcher de progresser à l'échelle européenne. Dès lors, en l'absence de progrès suffisants à l'échelle internationale, ils estiment qu'il conviendra d'appliquer les solutions adéquates à l'échelle européenne, éventuellement dans le champ d'application de l'ACCIS, ou par le biais d'un véhicule législatif spécifique.

EXAMEN EN COMMISSION

La Commission s'est réunie le 6 décembre 2017, sous la présidence de Mme Sabine Thillaye, Présidente, pour examiner le présent rapport d'information.

L'exposé du rapporteur a été suivi d'un débat.

Mme la Présidente Sabine Thillaye. Mes chers collègues, le marché unique du numérique constitue l'une des priorités majeure de la présidence estonienne. Il s'agit également pour la France d'une priorité de premier ordre. Je souhaite que la question du numérique imprègne l'ensemble de nos travaux dans une logique prospective. La révolution numérique modifie de fond en comble les manières de penser, de communiquer, de produire. Notre plus grand défi est de penser le monde qui vient et d'anticiper les innovations de rupture que sont la transformation numérique et l'intelligence artificielle. Si elle a manqué la première révolution numérique au profit de compagnies presque exclusivement américaines et asiatiques, l'Europe doit se positionner à l'avant-garde des innovations technologiques. Plutôt que de subir ces transformations, impassibles, nous devons affirmer un « modèle européen » qui nous soit propre. Notre diversité de perceptions, de cultures et d'approches doit être mise au profit d'une Europe de l'innovation. L'interculturalité doit constituer un vecteur d'innovation et de progrès, afin de nous permettre d'être à l'avant-garde de la révolution numérique. Je vous rappelle qu'une Conférence sur ce sujet sera organisée à l'Hôtel de Lassay demain de 14 h 30 à 18 h 30 en présence du Vice-président de la Commission européenne en charge du numérique, M. Ansip, et du secrétaire d'État chargé du numérique, M. Mahjoubi, ainsi que de représentants de la société civile et d'entrepreneurs du numérique. Nos deux co-rapporteurs y présenteront leurs travaux. Vous y êtes les bienvenus.

Je passe la parole à M. Éric Bothorel et à Mme Constance Le Grip pour présenter leur rapport, ainsi que leur proposition de résolution.

Mme Constance le Grip, co-rapporteure. Nous avons le plaisir de vous présenter le fruit de notre travail commun sur le marché unique du numérique. La proposition de résolution européenne qui vous est soumise aujourd'hui traite du marché unique du numérique. Il s'agit en effet d'un effort de longue date que mène la Commission Juncker, qui avait fait du numérique l'un des dix grands chantiers de la période 2014-2019. L'objectif de la Commission était de libérer le potentiel de croissance, de recherche, d'intelligence collective de l'Union européenne en la matière et de faire de l'Union européenne un champion du numérique. Nous avons souhaité, avec M. Bothorel, vous rendre compte de l'avancée des travaux au sein des institutions européennes, sur les différents aspects de la législation européenne en cours d'élaboration. Sous la précédente mandature, la Commission des affaires européennes de l'Assemblée nationale

avait déjà eu l'occasion de traiter des aspects essentiels de la révolution numérique en cours et de ses incidences sur un certain nombre de politiques publiques. Devant l'ampleur de la tâche, nous avons souhaité nous concentrer sur quatre aspects saillants de l'ensemble de la stratégie de la Commission européenne en vue de l'établissement d'un marché unique du numérique. Nous voulons apporter des éléments d'information que nous espérons nouveaux et surtout utiles dans la perspective des travaux que nous serons amenés à mener au sein de l'Assemblée nationale.

La plus grande partie de cet effort a d'abord été réservée à la suppression des obstacles nationaux, réglementaires ou techniques, dont il était estimé qu'ils contrevenaient au bon fonctionnement du marché intérieur dans le secteur du numérique. La Commission européenne a pris conscience d'un ensemble de facteurs, tels que le poids des plateformes dans l'économie actuelle, qui confine parfois à la formation de monopoles, ou la capacité des entreprises numériques, en vertu de la légèreté de leurs structures, à profiter des écarts en matière d'impôt sur les sociétés entre les différents États membres. À côté des efforts pour aplanir les obstacles à la création d'un véritable marché européen du numérique est apparue la nécessité d'avoir une activité régulatrice pour accompagner et si possible prévenir un certain nombre de ces phénomènes mondiaux, auxquels je fais référence. Il s'agit de garantir des libertés fondamentales, telles que la protection de la vie privée, la protection des données personnelles et du caractère privé des correspondances. Cette activité de régulation s'est ajoutée à la suppression des obstacles nationaux à la réalisation du marché intérieur.

Ce double prisme ressort des textes que nous avons examinés au cours de cette mission, pendant laquelle nous avons eu l'occasion de prendre en compte les avis de nombreux acteurs privés et publics, à Paris comme à Bruxelles. Nous nous sommes penchés sur la proposition de règlement relative à la libre circulation des données non-personnelles (ou *Free flow of Data*). C'est un élément de législation très important, actuellement en cours d'examen au sein des instances européennes. Nous allons également – et c'est sur ces sujets que nous avons bâti nos propositions au sein de la résolution européenne – aborder la question de l'encadrement des données personnelles. Le troisième sujet que nous traitons est essentiel, d'une importance vitale pour nos économies et nos modèles de société : la cybersécurité pour les services numériques sur le continent européen et les échanges entre acteurs numériques sur le continent. Dernier axe de travail : l'initiative de la France et d'autres pays de l'Union européenne pour une fiscalité numérique juste.

Le projet de règlement sur la libre circulation des données non-personnelles est le premier objet dont nous nous sommes emparés. Quand on parle de marché européen du numérique, on pense assez rapidement à la libre circulation. C'est en effet avec la suppression d'obstacles nationaux injustifiés que les entreprises européennes peuvent disposer d'un ensemble de données propice à leur croissance, permettant de soutenir la concurrence féroce des entreprises américaines et chinoises. Nous avons besoin que la croissance d'un certain

nombre de nos petits, moyens et grands acteurs économiques puisse se faire en disposant d'ensembles de données pertinents, importants, ainsi que des algorithmes adéquats. Il faut parachever le dispositif européen, en mesure tous les tenants et aboutissants avant que de songer à intégrer les données non-personnelles au sein des accords commerciaux avec d'autres zones du monde actuellement en projet.

M. Éric Bothorel, co-rapporteur. Nous avons dû travailler un champ extrêmement vaste, à des fins de réalisation du rapport et de la proposition de résolution qui vous est soumise. Nous avons assumé des choix. Certains regretteront peut-être que nous ne soyons pas allés assez loin sur le droit d'auteur, d'autres nous reprocheront de ne pas avoir traité tel ou tel sujet. Compte tenu du nombre de personnes à auditionner pour aboutir à une position équilibrée entre sécurité et libertés individuelles, les propositions que nous formulons ce soir sont en droite ligne avec l'intention première qu'il faut rappeler : la nécessité de faire émerger le marché unique du numérique. Celui-ci permettrait de faire naître des acteurs européens de premier plan dans le monde du numérique.

Cette libre circulation doit notamment se traduire par une obligation aussi faible que possible de localiser les données dans des *data center* nationaux, sinon pour des raisons légitimes de sécurité nationale. Certains ont peut-être à l'esprit l'initiative française du *cloud* souverain, elle s'est traduite par des difficultés pour un certain nombre de directeurs de systèmes d'information, pour maintenir les données sur le territoire français.

À l'inverse, l'Allemagne vient de tenter une expérimentation avec un duo entre *Deutsche Telekom* et *Microsoft* pour l'hébergement de données en Allemagne et l'encapsulation de ces mêmes données rendues inaccessibles par ces deux entreprises. On le voit, les questions de libre circulation des données et de leur localisation ne doivent pas répondre au seul critère de la géographie, mais aussi à des dimensions technologiques et techniques. L'économie des nuages, en particulier, se soumet aussi peu aux frontières nationales que les nuages eux-mêmes, physiques ou numériques. En contrepoint, toutefois, les autorités nationales doivent pouvoir, par le biais d'une collaboration efficace, avoir accès aux données non-personnelles à tout moment, dès lors que cet accès est justifié par un intérêt public suffisant. De la même manière, les internautes doivent pouvoir bénéficier de cette libre circulation des données afin de récupérer les données générées par l'utilisation d'un service et les transférer facilement auprès d'autres prestataires. On a vu là aussi des initiatives nationales sur la portabilité des données et la possibilité de changer d'opérateur de manière totalement transparente. La proposition de règlement destinée à protéger les données personnelles échangées par le biais des télécommunications, dite « *ePrivacy* », constitue, quant à elle, ce que l'on pourrait appeler une *lex specialis* de l'ensemble plus large que constitue le Règlement Général de Protection des Données, ou RGPD. Celui-ci doit garantir le niveau le plus élevé au monde de protection des données personnelles dans tous les secteurs. Nos entretiens nous ont toutefois amenés à faire les constats suivants :

- la conformité au RGPD réclame de la part de nombreuses entreprises, mais aussi de collectivités publiques, un effort d'adaptation, qui n'est encore que trop rarement effectif. Or, l'application du RGPD est prévue au 25 mai 2018 : cette conformité s'avère naturellement plus difficile pour les petites entreprises que pour les grandes, qui ont à la fois la force de frappe juridique et le personnel formé pour mettre en œuvre ces adaptations. Il va sans dire qu'un groupe de 500 personnes a toujours la possibilité de trouver quelque part quelqu'un à former pour devenir *chief data officer*. Pour une entreprise de dix, quinze ou trente salariés, dont le cœur d'activité n'est pas de se mettre en conformité avec tel ou tel type de règlement, mais de développer ses activités, qu'elles soient d'entreprise à entreprise ou d'entreprise à client, le temps et les ressources disponibles sont très difficiles à mobiliser.

- La succession d'un certain nombre de règlements qui s'appliquent, du RGPD à, demain, *ePrivacy*, suscite des interrogations, tant sur les ressources à y allouer pour se mettre en conformité que sur l'incertitude juridique issue des révisions successives. Il faut développer notre vigilance, pour améliorer la prévisibilité et la cohérence, loin des injonctions contradictoires entre diverses réglementations.

- Il devient de plus en plus urgent d'intégrer, comme le préconise la CNIL depuis un certain temps, les marges de manœuvre contenues dans le RGPD pour les États membres dans un véhicule législatif adapté, qui doit produire ses pleins effets au 25 mai 2018.

N'ayons pas une vision trop pessimiste de ce que représente le RGPD. Après les auditions que nous avons menées, ainsi que les rencontres dans les territoires et les circonscriptions, avec des chefs d'entreprise et des acteurs économiques, tout le monde se félicite de l'orientation prise par l'Union européenne en faveur de la défense et la protection des données. Rien ne dit que la tendance dictée par d'autres opérateurs transcontinentaux sur le fonctionnement du traitement des données et de leur marchandisation représente l'avenir. Je suis pour ma part convaincu qu'avec le RGPD, on verra de plus en plus d'opérateurs, y compris extracontinentaux, se plier à ces règles. Des sensibilités comparables émergent aux États-Unis et à l'Est de la planète.

Plus largement, le consentement, tel qu'il est compris dans le RGPD, doit irriguer le règlement *ePrivacy*. C'est en ce sens que nous demandons à ce que le consentement de l'utilisateur ne soit pas présumé en amont par le paramétrage automatique du navigateur, mais qu'il soit recueilli, notamment pour ce qui est des « cookies tiers », après une information claire de l'utilisateur. Aujourd'hui, l'internaute est sollicité et informé du type d'information recueillie sur une page web. Il y a deux catégories d'utilisateurs : ceux qui cochent pour avoir accès à l'ensemble des services, sans trop savoir à quoi ils s'exposent et ceux qui, par habitude ou par conviction, ne souhaitent pas laisser de traces sur internet. Ils peuvent alors décider de ne pas aller plus loin ou ne pas accepter le traçage. Nous

souhaitons, par nos propositions, déplacer le curseur, aujourd'hui très favorable à ceux qui savent, vers ceux qui ne savent pas, pour les informer, non pas des risques, mais des sujets auxquels ils s'exposent demain, tels que le profilage, ou la différence dans le traitement de l'information.

Nous aurions, en matière de cybersécurité, bien plus de réserves sur le texte proposé par la Commission européenne, au milieu d'un ensemble qui compose le « paquet cybersécurité ». La proposition de règlement accroît le mandat de l'ENISA, soit l'agence européenne de cybersécurité et lui confie notamment la gestion d'un système de certification européen. Ces deux points peuvent poser problème.

En premier lieu, les agences nationales comme l'Agence nationale de la sécurité des systèmes d'information (ANSSI) en France ont démontré depuis de nombreuses années leurs capacités à assurer la cybersécurité des citoyens dans les États membres. Dès lors, un accroissement du mandat de l'ENISA, qui ne dispose par ailleurs que d'un personnel limité, ne doit pas se faire au détriment de la capacité d'action de chacune des autorités nationales. L'ANSSI compte 500 agents, contre 80 à l'ENISA. Cela ne doit pas décourager non plus les États membres dépourvus d'une autorité comparable à l'ANSSI d'investir dans leur cybersécurité. De plus, les schémas de certification nationaux, tels que celui défini par l'ANSSI pour la France, sont déjà reconnus parmi les meilleurs standards mondiaux. Dès lors, une certification européenne doit viser un niveau ambitieux, tout en modulant le degré de certification en fonction du caractère stratégique des objets concernés.

Enfin, et nous en terminerons par-là, la fiscalité qui s'applique aux entreprises numériques doit viser une plus grande justice et une meilleure efficacité. Je ne reviendrai pas sur les nombreux cas qui ont émaillé l'actualité ni sur la définition toute récente par la Commission européenne d'une nouvelle liste de paradis fiscaux. Mais les caractéristiques de l'économie numérique sont propices aux risques d'érosion de la base fiscale et de transfert des bénéfices, en vertu de la légèreté des actifs engagés, de l'absence d'infrastructures physiques dans les pays dans lesquels la valeur ajoutée est créée ou encore de la possibilité de s'implanter dans des États tout en exerçant une majeure partie de son activité ailleurs. C'est cet état de fait que le Gouvernement français a souhaité corriger avec sa proposition d'une taxe d'égalisation, portant sur le chiffre d'affaires des entreprises du numérique dans chaque État membre. Le but est véritablement de taxer la valeur là où elle est créée, et ce d'autant plus que les acteurs du numérique ont besoin de biens publics, tels que des infrastructures de bonne qualité ou une main-d'œuvre qualifiée. C'est à ce titre, entre autres, qu'une juste contribution nous paraît indispensable. Cette taxe ne sera toutefois qu'un premier pas avant la conclusion des travaux de l'OCDE en la matière, au printemps 2018. Mais des progrès rapides sur ces sujets permettront à l'Union européenne d'avoir une position commune et donc de peser d'autant plus dans les débats mondiaux à venir relatifs à l'impôt sur les sociétés.

Mme la présidente Sabine Thillaye. Avant de passer aux questions, je me permets de saluer et d'accueillir dans notre commission, M. Raphaël Schellenberger qui vient en remplacement de M. Marc Le Fur.

Mme Sophie Auconie. Madame la Présidente, chers collègues. J'interviens au nom de Laure de La Raudière qui, en appui de la mission confiée à M. Villani sur l'intelligence artificielle, a travaillé sur ce sujet. Elle me demande de vous transmettre quelques réflexions par rapport à votre présentation. Elle proposera des amendements à l'occasion de l'étude de cette proposition de résolution par la commission des affaires économiques. Au neuvième considérant, l'obligation de stockage des données sur le territoire européen pour des considérations nationales ou européennes mérite sans doute d'être expertisée et débattue plus longuement. Mme de La Raudière est ennuyée que la proposition réfute son éventuel intérêt et préférerait que ce considérant soit retiré. Il n'est d'ailleurs pas indispensable à la proposition de résolution européenne. De plus, dans ce même paragraphe, la proposition dit une chose et son contraire à la ligne suivante. La suppression de cette partie semble sage. Au dixième considérant, elle souhaite entendre vos explications. Au onzième considérant, elle indique qu'elle est tout à fait en faveur de la portabilité des données personnelles et que c'est d'ailleurs inclus dans le RGPD. En revanche, la définition des données enrichies par le fournisseur de service n'est pas claire ; il serait utile de la préciser. Elle pense qu'il faudrait supprimer la mention « à l'exclusion des données enrichies par le fournisseur de service » et en rester au principe de changement de fournisseur de service et de portabilité des données, parce qu'il s'agit d'une proposition de résolution et non un texte de loi. Le point 8 de la proposition de résolution n'est pas clair et nécessite des explications. Enfin, le point 10 est problématique et nous avons eu de nombreux débats sur ce sujet au moment de la loi pour une République numérique. Les données générées par l'utilisation du service ne doivent pas inclure les secrets de fabrication de l'entreprise et cela mérite d'être précisé. Elle vous remercie de votre écoute.

M. Éric Bothorel, co-rapporteur. Vos remarques portent sur des éléments rédactionnels ou de précision qui me paraissent pour certains utiles, notamment sur les données enrichies. Nous avons eu ce débat pendant la loi sur la République numérique. Je connais les instances qui portent ce type de sujet et je ne vois aucun inconvénient à ce qu'il y ait des amendements rédactionnels ou de précision sur ces points-là.

Mme Constance Le Grip, co-rapporteure. Pour les éléments cités, cela ne nous semble pas contradictoire. Ce sera peut-être un débat qu'il faudra approfondir à d'autres occasions, mais il peut y avoir des cas expressément justifiés et identifiés de localisation forcée des données, par exemple pour des raisons de sécurité ou de défense. Mais cela ne doit pas empêcher que la libre circulation se fasse via un principe de libre coopération reposant sur une collaboration étroite entre les autorités nationales.

M. Éric Bothorel, co-rapporteur. On introduit l'idée qu'il y a une règle générale et une exception, mais l'exception ne peut pas devenir la règle. Je rappelais cela notamment avec la notion de *cloud* souverain où on avait dit *de facto* que toutes les collectivités publiques devaient faire appel à des fournisseurs de services qui offraient la garantie d'un *cloud* souverain. Dit autrement, les données restaient sur le territoire national. C'est une traduction technique dont on avait du mal à trouver la réalité en France et, en vérité, il y avait très peu de fournisseurs qui étaient en capacité de dire où les données étaient localisées. Ce n'est pas parce qu'un *data center* est localisé en France qu'on a la garantie que les données et leur traitement restent en France. Ce que l'on expose dans la proposition de résolution, c'est de s'inscrire dans une logique de libre circulation des données à l'échelon du continent européen, n'exceptant pas l'idée que pour des raisons particulières, il faille les conserver sur le territoire national. Comme le disait Mme Le Grip tout à l'heure, nous nous trouvons devant des enjeux d'intelligence artificielle : la performance de l'algorithme est liée à la taille des *data sets*. Soit vous voulez des entreprises qui sont performantes et donc vous leur offrez la possibilité d'avoir accès à de larges quantités de données : cela nécessiterait un débat sur l'anonymisation et la pseudonymisation des données. Soit on réduit le terrain de jeu de l'ensemble des acteurs économiques au territoire national. Aujourd'hui, je pense à *Facebook* qui a deux cents millions d'utilisateurs aux États-Unis. Avec cette base, ils ont une large capacité de développement des algorithmes comportementaux et *marketing*. Si on restreignait l'utilisation d'un certain nombre de données, notamment les données publiques, qui une fois anonymisées ou pseudonymisées, pourraient servir dans le domaine de la santé, on réduirait la possibilité d'innover. Il faut prévoir des limites ; il faut prévoir des exceptions, si on décide qu'un certain nombre de données n'ont pas, pour des raisons de secret industriel ou de protection nationale, à circuler librement. Donc il n'y a pas de contradiction. Dans la rédaction d'une proposition de résolution, il est difficile de faire tenir tous ces éléments de précision. Pour le reste, si tôt la commission saisie sur le fond, il sera apporté des réponses.

M. Thierry Michels. Je salue à mon tour l'excellent travail des rapporteurs sur ce sujet essentiel. Dans cette société de la connaissance, la circulation va de pair avec la protection des données pour garantir la confiance des citoyens européens. Or plusieurs incidents ont récemment montré que les acteurs n'étaient pas forcément vertueux, qu'il s'agisse d'Uber dont 60 millions de données de conducteurs et d'utilisateurs ont été dérobées, ou bien de la poupée Cayla, manipulable à distance. Un robuste volet cybersécurité est donc indispensable si l'on veut renforcer la confiance des citoyens dans le partage des informations. C'est essentiel pour bénéficier des innovations offertes par l'exploitation des données, par exemple en matière de télémédecine ou bien de réseaux énergétiques intelligents, mais cela suscite des craintes - sur ce point, voyez les difficultés rencontrées par le déploiement du compteur Linky. Considérez-vous que les moyens des organismes tels que la CNIL sont suffisamment renforcés par ces avancées ?

M. Pieyre-Alexandre Anglade. La France a tardé à s'emparer de ce sujet pourtant très important, au point d'apparaître à la remorque, finalement, d'autres États membres et d'autres instances européennes. Ce projet de règlement favorise la libre circulation des données non personnelles, interdit les géoblocages injustifiés imposés par les États sur leur territoire, ménage des exceptions de bon sens pour les données relatives à la sécurité publique. La France porte, au Conseil, une extension de ces exceptions aux données administratives, notamment de santé publique. En effet, la libre circulation des données nécessite une confiance absolue tant envers l'État membre concerné qu'envers les citoyens, qui parfois n'existe pas. Que pensez-vous de cette proposition française d'extension de l'exception aux données administratives ?

M. Raphaël Schellenberger. Ce sujet est très vaste, et parmi les nombreuses questions qu'il pose, il y a celle du droit d'auteur. Le marché unique est finalement un outil de développement économique de notre espace commun face à d'autres grandes zones, qui nous font concurrence. Dans certaines zones, des règles plus souples en matière de droits d'auteur favorisent les acteurs économiques. Ne risque-t-on pas, avec ces règles proposées d'une façon un peu trop légère sous le prisme du marché unique du numérique, un *dumping* au sein de l'Union européenne ?

Mme Constance Le Grip, co-rapporteure. Sur le droit d'auteur, M. Schellenberger, nous l'abordons aux points 18 et 19 de la proposition de résolution européenne : c'est un sujet loin d'être anodin, mais ce n'est pas le cœur de notre rapport. La commission des affaires européennes a traité ce sujet sous la précédente législature avec l'excellent rapport Gaymard-Karamanli sur l'adaptation du droit d'auteur à l'ère numérique. Notre Assemblée, *via* notamment la commission des affaires culturelles, suit très attentivement la finalisation en cours de la révision de la directive sur le droit d'auteur, et le Gouvernement comme les eurodéputés français sont très engagés pour que l'harmonisation des règles du droit d'auteur ne se traduise pas par un amoindrissement de ce dernier, mais bien au contraire par son renforcement. C'est un droit moderne, car immatériel, parfaitement adapté à cette révolution numérique. De la même façon, sans en faire le cœur du rapport, nous avons parlé d'autres sujets, évoqués à juste titre notamment par Mme Sophie Auconie relayant les préoccupations de Mme de La Raudière, comme le secret de fabrication, le secret d'affaires, la propriété intellectuelle, etc., pour lesquels se posent des questions similaires de lutte contre la contrefaçon, le piratage.

M. Éric Bothorel, co-rapporteur. Vos rapporteurs ne sont pas favorables à l'extension de la localisation à d'autres natures de données car une réflexion en silo avec les données de sécurité, les données de santé, etc., comporte le risque d'aboutir à une restriction trop forte de la circulation des données. Une approche plus fine permet de définir ce qu'est une donnée sensible ou pas, protégée ou pas. Faut-il avoir une approche globale ou bien une approche différenciée en fonction de telle ou telle nature de données ? La première approche est celle qui a été suivie jusqu'à présent, en considérant qu'une entreprise, un *process*, un ensemble de

données devaient être protégés. Mais il y a des opérateurs d'importance vitale (OIV) qui produisent des données qui ne sont pas des données sensibles. Compte tenu de cette dualité, vos rapporteurs considèrent qu'il faut avoir une autre approche, en se donnant autant que faire se peut les moyens d'assurer la liberté de circulation des données la plus grande possible en Europe, ce qui implique de renforcer la coopération entre les États membres et notamment entre leurs agences.

Le cas de l'Estonie est éclairant. Ce pays, très avancé en matière d'économie numérique, a fait le choix d'abriter ses données au Royaume-Uni, considérant que leur protection y était mieux assurée qu'en Estonie même. Les choix de protection des données ne répondent pas, parmi les États membres, à des critères identiques.

S'agissant de la Commission nationale de l'informatique et des libertés (CNIL) et des autres autorités, comme l'Agence nationale de la sécurité des systèmes d'information (ANSSI), au-delà des moyens humains nécessaires pour conduire leurs actions, les dispositions réglementaires, notamment pour ce qui est des sanctions, sont par elles-mêmes dissuasives et devraient entraîner la mise en conformité des entreprises à ce règlement.

Sur le sujet de la confiance, qui est essentielle, vous avez raison, M. Michels : cette dernière repose à mon sens sur la transparence et l'accès aux données, c'est-à-dire que le consommateur d'une montre connectée, d'une poupée connectée, de domotique est informé non seulement des services rendus par ces outils, mais surtout des données captées. Ce consommateur doit savoir à qui elles sont destinées, s'il s'agit d'un tiers connu ou inconnu. Les fournisseurs doivent être dans l'obligation de donner l'information la plus claire possible sur l'intention sous-jacente au recueil des données.

Mme Constance Le Grip, co-rapporteure. Cela pose aussi la question de la certification des objets connectés, et du niveau de cette dernière, au plan européen, par l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) ou bien au plan national pour les États membres qui ont cette capacité, comme la France et l'Allemagne.

Mme Marietta Karamanli. Les enjeux ne sont pas nouveaux, notamment pour les données personnelles, le droit d'auteur, la stratégie à avoir tant au niveau des États membres qu'au niveau de l'Union. Je me félicite de la continuité des travaux de notre commission, qui s'était déjà penchée sur ce dernier sujet en février dernier.

Il me semble que, en cohérence avec la préoccupation traditionnelle de la France, la proposition de résolution européenne devrait insister plus fortement sur deux éléments clés du modèle économique : d'une part, la question de la régulation des plateformes, essentielle non seulement pour maintenir les services, créer de la confiance, mais aussi pour lutter contre les nouveaux monopoles

qu'elles génèrent et, d'autre part, garantir la propriété des données collectées, c'est-à-dire, le droit pour les personnes d'y consentir, d'y accéder, de les récupérer, de les faire effacer, c'est-à-dire le droit à l'oubli.

En matière de cybersécurité, je partage votre analyse au sujet du renforcement de la coopération des agences, mais j'ajouterai un point important, celui du contrôle des agences, notamment le contrôle parlementaire. Nous en avons parlé lors de notre discussion sur Europol.

M. Bernard Deflesselles. Je partage l'appréciation flatteuse de mes collègues sur ce rapport. Pourriez-vous toutefois nous préciser le contenu des règles en matière de sécurité et de sûreté des données numériques que vous appelez de vos vœux aux points 8 et 9, ainsi que ce que devrait être l'articulation entre l'action des agences au niveau européen et au niveau des États membres, dont vous parlez au point 14 ?

Mme Danièle Obono. Le numérique permet de futures révolutions technologiques, mais aussi démocratiques. Il est donc crucial que l'Europe soit à l'avant-garde. Mais ce projet de règlement général me semble surtout légaliser les stratégies d'entreprises privées, dont les collectes de données personnelles à des fins commerciales avec notamment le profilage, sont antagonistes avec l'idée même de démocratisation. Nous sommes favorables à une telle collecte lorsqu'elle se fait à des fins artistiques, de recherche, ou dans un sens d'intérêt général.

Je partage votre position sur la nécessité de défendre les agences nationales de protection : or ce règlement renforce le niveau européen. Que faire ? Il limite fortement le droit à l'oubli, alors que nous voulons au contraire le protéger. Comment faire ?

Quant à la taxation des entreprises du numérique, plusieurs démarches, parfois contradictoires d'ailleurs, ont été lancées par la Commission et par la France, vous l'avez évoqué. Quel est votre point de vue sur la proposition française, notamment sur la taxation des entreprises déficitaires et la définition du périmètre des entreprises numériques, alors que l'Assiette Commune Consolidée pour l'Impôt sur les Sociétés (ACCIS) a un champ plus large, avec ses trois indicateurs d'activité ? Quel projet devrait être mis en œuvre de façon prioritaire ? Les attentes de nos concitoyens sont fortes, tant au regard de l'enjeu démocratique que des recettes fiscales qui en découlent !

M. Bruno Gollnisch, membre français du Parlement européen. Je souhaiterais réagir aux propos de la Rapporteure, Mme Constance Le Grip sur le positionnement que pourraient avoir les institutions européennes et aussi nationales au sujet de la limitation de la liberté d'expression, notamment la répression de l'incitation à la haine. Nous sommes tous attachés à la liberté d'expression et nous sommes tous d'accord pour que celle-ci s'exerce dans les limites fixées par le code pénal. L'appel à la commission d'un crime ou d'un délit ne doit pas être possible, quel que soit le mode de transmission des données. La

difficulté vient du flou qui entoure le concept de haine, qui n'est jamais déterminé de manière précise. La haine est un sentiment, certes répréhensible mais également insusceptible de mesure. La définition qui en est faite peut être extrêmement variable. « *Selon que vous serez puissant ou misérable, les jugements de cour vous rendront blanc ou noir* ». Un discours pourra être qualifié d'incitation à la haine, alors que le discours opposé, s'il émane d'un groupe majoritaire ou exerçant le pouvoir, sera qualifié de discours d'amour, de justice et de vérité. C'est un problème. De manière identique, une même caricature ne sera pas appréciée de la même façon selon qu'elle émane de *Charlie Hebdo* qui, compte tenu des événements dramatiques qui l'ont frappé, est extrêmement bien vu des autorités, ou de M. Alain Soral. Je suis très attaché à ce que la loi soit la même pour tous et je tiens à faire part de mon inquiétude à ce sujet. Je crains que l'exploitation d'un sentiment diffus puisse permettre de museler la liberté d'expression de certains et favorise la domination doctrinale et culturelle de leurs opposants.

M. Éric Bothorel, co-rapporteur. Le champ du numérique est vaste. Nous n'avons pas abordé dans notre rapport des sujets tels que la cyber-malveillance, le cyber-harcèlement, les problématiques de la théorie du complot ou des rumeurs. L'Assemblée nationale a déjà légiféré à ce sujet et des missions d'information se sont penchées sur ces thématiques. Mais une actualisation est peut-être nécessaire et cela justifierait que certaines commissions parlementaires engagent une nouvelle réflexion sur ces thèmes.

Je pense qu'Internet n'est pas à l'origine de la diffusion d'informations malveillantes mais qu'il constitue une caisse de résonnance inédite en vertu d'une capacité extraordinaire de massification de l'information. C'est un outil capable de créer des biais de connaissance autour desquels se forment des communautés. Il permet à des petits groupes de mobiliser une idéologie et de l'imposer aux autres. Ce sont ces dangers auxquels nous devons faire face. Gérald Bronner dans *La démocratie des crédules* met en évidence la vulnérabilité de la société à ce sujet. Certains estiment peut-être que la régulation des plateformes pourrait permettre d'effectuer un tri entre la bonne information et la mauvaise. Il ne serait pas malsain d'avoir un débat sur les « *fake news* » ou sur la hiérarchisation des informations. Mais je pense qu'au-delà de la régulation des plateformes, ce à quoi nous sommes tous très attachés, c'est surtout la possibilité d'avoir accès de manière transparente aux algorithmes qui permettent de hiérarchiser les informations. Pourquoi lorsque l'on tape « bébé » sur *Google*, en Europe, n'apparaissent quasiment que des photographies d'enfants blancs ?

Les législateurs, nationaux et européens, doivent instaurer un cadre de liberté suffisant pour permettre l'innovation et la création de nouvelles formes de marchés, mais disposant de règles de veille et de contrôle permettant à tout moment de comprendre pourquoi l'utilisateur d'Internet se voit proposer tel produit. Le législateur, qui peut devenir régulateur, doit avoir accès aux outils qui hiérarchisent, concatènent et organisent l'information.

La question de la fiscalité des plateformes se pose depuis longtemps. Des initiatives, notamment une initiative française, ont été portées à ce sujet il y a quelques mois. Elles n'ont pas encore abouti mais il y a une avancée certaine et ce qui était inconcevable, à savoir la taxation des activités des plateformes sur le chiffre d'affaires réalisé dans chaque pays, est aujourd'hui discuté par des pays importants au sein de l'Union européenne. Je veux croire que ces efforts solidaires aboutiront rapidement à une solution.

Mme la présidente Sabine Thillaye. Il est beaucoup question de confiance dans les thématiques liées au numérique mais les entreprises continuent à recourir à des stratégies de contournement. Depuis l'arrêt Schrems, du nom d'un ressortissant autrichien qui avait obtenu gain de cause face à *Facebook*, *Google* donne à ses utilisateurs la possibilité de cocher les données qu'ils souhaitent ou ne souhaitent pas voir transférées, mais il faut réitérer cette manipulation tous les quinze jours. Des projets de sanctions sont-ils envisagés pour empêcher ce type de stratégies qui misent sur l'usure du consommateur ?

M. Éric Bothorel, co-rapporteur. Ces désagréments sont hélas répandus. C'est la raison pour laquelle nous proposons dans notre rapport de retenir une notion du consentement qui irait au-delà d'un simple « *opt out* », pour empêcher que les entreprises puissent considérer qu'une absence de renonciation catégorique vaut acceptation.

Mme la présidente Sabine Thillaye. Merci. La discussion générale est close. Nous passons à l'examen de la proposition de résolution. Nous sommes saisis de plusieurs amendements. Nous commençons par l'amendement n° 1 de M. Bothorel.

M. Éric Bothorel, co-rapporteur. Cet amendement rédactionnel vise à reprendre les termes de la CNIL dans la proposition de résolution.

Mme Constance Le Grip. Avis favorable.

L'amendement n° 1 est adopté.

L'amendement n° 2 est également présenté par M. Bothorel.

M. Éric Bothorel, co-rapporteur. Cet amendement rédactionnel vise à remplacer le mot « agence » par le mot « autorité » pour tenir compte du fait que la CNIL n'est pas une agence.

Mme Constance Le Grip, co-rapporteure. Avis favorable.

L'amendement n° 2 est adopté.

L'amendement n° 3 est présenté par M^{me} Karamanli.

Mme Marietta Karamanli. Cet amendement vise à préciser que l'harmonisation maximale mentionnée dans la proposition doit se faire « par le haut ».

Mme Constance Le Grip, co-rapporteure. Nous ne sommes pas convaincus que l'on puisse apporter cette précision car cela pourrait contrevenir aux marges de manœuvres dont devront pouvoir disposer les États membres lorsqu'ils traduiront dans leur droit interne les orientations générales contenues dans le règlement général sur la protection des données.

Mme Marietta Karamanli. Je tiens à vous rassurer. Nous sommes dans le cadre de l'examen d'une proposition de résolution, pas dans celui de la rédaction d'un règlement ou d'une directive.

M. Éric Bothorel, co-rapporteur. Une proposition de résolution n'est pas une succession de points désolidarisés les uns des autres. Il est évident que la proposition de résolution que nous vous soumettons est ambitieuse et il me semble inutile d'apporter cette précision.

M. Jérôme Lambert. Qui peut le plus, peut le moins. De plus nous sommes tous d'accord sur ce point. Alors pourquoi ne pas l'indiquer ?

Mme Constance Le Grip, co-rapporteure. À titre de prise de position politique et dans la mesure où cela n'interfère pas sur la rédaction du règlement général, je pense que l'on peut effectivement faire figurer cette précision.

M. Éric Bothorel, co-rapporteur. Je n'y suis pas opposé et cela permettra d'affirmer sans ambiguïté notre position commune.

Mme Marietta Karamanli. Je rappelle que dans cette commission nous avons toujours fonctionné de manière unanime avec la volonté partagée et profonde d'œuvrer en faveur de nos concitoyens et en rejetant tout positionnement politicien.

L'amendement n° 3 est adopté.

Mme la présidente Sabine Thillaye. Nous sommes saisis d'un amendement n° 4 présenté par M. Éric Bothorel, co-rapporteur.

M. Éric Bothorel, co-rapporteur. C'est un amendement qui vise à affirmer que, sans aller jusqu'à l'exclusivité, la conservation des données par les autorités publiques doit obéir en premier lieu à des fins expresses de sécurité et de défense nationale. Nous avons eu ce débat tout à l'heure pour savoir jusqu'où aller dans la collecte des données. C'est une modification qui n'emportera pas de gros sujet.

L'amendement n° 4 est adopté.

Nous sommes saisis d'un amendement n° 5 présenté par Mme Marietta Karamanli.

Mme Marietta Karamanli. Sur le point 7 de la proposition de résolution européenne, nous demandons de garantir aux internautes le droit d'exprimer un consentement libre. C'est un élément essentiel que vous rappelez mais nous pensons que la seconde partie de la phrase contraint le consentement libre. Nous proposons donc de supprimer cette partie de la phrase et s'en tenir à l'affirmation du principe du consentement libre des internautes sur le traitement des données.

M. Éric Bothorel, co-rapporteur. Je comprends la motivation et l'exposé des motifs de cet amendement. Il y a une singularité et une actualité autour du monde de la presse qui motive le positionnement de la proposition rédactionnelle initiale. L'idée est de ne pas nuire à certains modèles économiques qui ne pourraient pas s'adapter aux dispositions que nous préconisons. Il me paraît responsable, à ce stade, que nous ayons cette position mesurée plutôt que d'exclure fermement cette possibilité.

M. Jérôme Lambert. Je vois dans ce point 7 tout et son contraire : nous sommes entièrement d'accord avec la première partie mais les nuances introduites dans la seconde partie pour exclure certaines activités me posent problème. Vous introduisez une exception mais qui va déterminer cette exception ? Il n'y a alors plus de garantie et c'est la raison pour laquelle je soutiens cet amendement.

M. Éric Bothorel, co-rapporteur. J'entends votre point de vue, je vous renverrais bien que nous ne faisons pas la loi et le sujet qui est le nôtre aujourd'hui est une proposition de résolution. J'ai exposé de manière transparente et claire les raisons de l'articulation et de la rédaction proposées : il s'agit de permettre une transition.

Mme la présidente Sabine Thillaye.

L'amendement n° 5 est adopté.

Nous sommes saisis d'un amendement n° 6 présenté par Mme Marietta Karamanli.

Mme Marietta Karamanli. Il est défendu.

M. Éric Bothorel, co-rapporteur. Le point 8 traite des données non personnelles et ne peut donc, au risque d'un contresens, viser la protection des données personnelles. Avis défavorable donc.

L'amendement n° 6 est rejeté.

Nous sommes saisis d'un amendement n° 7 présenté par Mme Marietta Karamanli.

Mme Marietta Karamanli. C'est un amendement qui demande au Gouvernement de s'engager fortement sur la régulation des plateformes numériques qui, si elles créent de nouveaux modèles économiques, ne doivent pour autant être autorisée à privatiser, au sens d'en prendre le contrôle, un certain nombre de services et de données. C'est un engagement qui est demandé au Gouvernement à travers une nouvelle rédaction du point 8.

M. Éric Bothorel, co-rapporteur. Il y a déjà beaucoup de textes qui visent à réguler les plateformes et notamment le règlement général de protection des données. Je rappelle qu'il y a actuellement des travaux effectués par la Commission européenne qui pourraient aboutir sur des propositions qu'il conviendra d'examiner en temps voulu.

Mme Marietta Karamanli. Il s'agit d'affirmer un peu plus la protection par rapport aux privatisations. C'est une protection que l'on ajoute au niveau de ce qui est proposé au point 8.

M. Éric Bothorel, co-rapporteur. Il faudrait alors préciser ce qu'on entend par privatisation donc j'y suis défavorable.

L'amendement n° 7 est rejeté.

Nous sommes saisis d'un dernier amendement n° 8 présenté par Mme Marietta Karamanli.

Mme Marietta Karamanli. Sur le point 17, la proposition consiste à ajouter, après les termes « *assiettes fiscales* » l'expression « *tout en travaillant à une harmonisation par le haut des taux d'imposition des services numériques* ». Cela rejoint le premier amendement que nous avons présenté et s'inscrit totalement dans une volonté d'harmoniser l'imposition fiscale qui est assez largement portée au sein de notre assemblée et également par le Gouvernement.

M. Éric Bothorel, co-rapporteur. Je suis embêté par cet amendement car nous ne sommes déjà pas parvenus à harmoniser la fiscalité dans l'économie réelle. Nous sommes, certes dans une proposition de résolution, mais également dans une démarche où on suit les travaux effectués par ailleurs dans le domaine fiscal. On a rappelé, tout à l'heure, le long chemin parcouru par l'idée d'aboutir à une fiscalité des activités numériques. Je crains que si l'on pose comme un point non-négociable la nécessité d'avoir à la fois une fiscalité et une harmonisation des taux pour le secteur numérique, on risque de n'aboutir à rien. Cela me semble être un obstacle supplémentaire à la réalisation d'une fiscalité du numérique. Nous portons tous les deux et, ensemble de manière plus générale, l'idée qu'il faut aller très vite et très loin sur la fiscalité des plateformes. Mais conditionner les avancées en la matière à une harmonisation par le haut me paraît être de nature à décourager les ambitions portées pour aboutir à une fiscalité du numérique.

M. Jérôme Lambert. Ce qui compte en Europe aujourd'hui, c'est l'harmonisation. Peu importe finalement la valeur du taux si on arrive à converger vers un taux plus cohérent pour tous les États membres.

Mme Danièle Obono. Je pense au contraire qu'aujourd'hui en Europe, ce n'est pas juste l'harmonisation mais l'harmonisation par le haut qui est importante. Si on ne donne pas de signal positif et ambitieux, en particulier sur le secteur d'avant-garde que représente le numérique, il me semble que l'on passe à côté d'une question cruciale. L'harmonisation dans un sens ou dans un autre n'a pas le même impact, notamment dans les consciences, sur l'image de l'Europe. Savoir si l'on se dirige vers une Europe du mieux ou du moins-disant fiscal et social n'est pas un détail insignifiant.

Mme Marietta Karamanli. Je tiens juste à rappeler le positionnement du Président de la République en matière d'harmonisation fiscale qui insiste fortement, depuis plusieurs mois, dans ses discours sur cette question. Si au sein même de la majorité cette volonté n'est pas portée dans une proposition de résolution, il me semble qu'il y a un recul…

M. Éric Bothorel, co-rapporteur. Il ne s'agit pas d'un recul, mes chers collègues. J'entends que l'on puisse nourrir des ambitions pour une fiscalité dans le secteur du numérique très fortes qui soient de réussir à faire avec le numérique tout ce que l'on n'a pas réussi à faire dans le reste de l'économie réelle. Il convient de rappeler les différences qui peuvent exister en matière de fiscalité ; aujourd'hui l'harmonie fiscale et l'harmonie sociale ne sont pas au rendez-vous. Je pense qu'il est illusoire de penser que parce qu'il s'agit de plateformes numériques, on arrivera à faire tout ça en même temps. À ce stade, cette double ambition me semble prématurée. Si les collègues ici présents s'associent à l'idée qu'on salue l'effort pour aboutir rapidement à une fiscalité des plateformes et des activités numériques, cela me semble déjà bien. Je partage l'idée selon laquelle l'Union européenne devrait, dans un monde idéal, avoir un mode de fonctionnement plus harmonieux mais à ce stade, portons la volonté d'avancer vite et bien sur la fiscalité du numérique, chose encore impensable il y a quelque temps, et nous traiterons ensuite de la capacité des uns et des autres à œuvrer pour son harmonisation.

M. Damien Pichereau. Je suis un peu gêné par cet amendement. Comme le rappelait Marietta Karamanli, l'harmonisation fiscale est un thème que j'ai pu porter pendant la campagne présidentielle et c'est notamment l'ambition du Président de la République. Ce qui me dérange, c'est la mention des termes « par le haut » car il ne s'agit pas de considérer que notre système d'imposition est le meilleur, ni même que l'imposition la plus haute est la meilleure. J'aimerais proposer de sous-amender éventuellement cet amendement pour supprimer ces termes.

Mme Marietta Karamanli. J'accepte ce sous-amendement.

M. Éric Bothorel, co-rapporteur. Pour satisfaire toutes les parties, je vous propose d'ajouter à la rédaction initiale l'idée d'harmonisation proposée par l'amendement sans mentionner les termes « par le haut ».

Mme la présidente Sabine Thillaye. Je mets aux voix l'amendement ainsi modifié : « *après les termes « assiettes fiscales », ajouter les termes « tout en visant une harmonisation des taux d'imposition des services numériques* ».

L'amendement n° 8 est adopté.

La proposition de résolution ainsi modifiée est adoptée.

PROPOSITION DE RÉSOLUTION EUROPÉENNE INITIALE

Article unique

L'Assemblée nationale,

Vu l'article 88-4 de la Constitution,

Vu les articles 16 et 114 du TFUE (Traité sur le fonctionnement de l'Union européenne),

Vu la directive n° 95/46/CE du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données,

Vu la directive n° 2002/58/CE 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 ;

Vu le règlement n° 2016/679 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),

Vu le règlement n° 526/2013 du 21 mai 2013 concernant l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) et abrogeant le règlement (CE) n° 460/2004,

Vu la Communication de la Commission européenne « Stratégie pour un marché unique numérique en Europe » du 6 mai 2015,

Vu la Communication de la Commission européenne « Créer une économie européenne fondée sur les données » du 10 janvier 2017,

Vu la proposition de règlement concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques et abrogeant la directive 2002/58/CE (règlement « vie privée et communications électroniques ») du 10 janvier 2017,

Vu la proposition de règlement concernant un cadre applicable à la libre circulation des données à caractère non personnel dans l'Union européenne du 13 septembre 2017,

Vu la proposition de règlement relatif à l'ENISA, Agence de l'Union européenne pour la cybersécurité, et abrogeant le règlement (UE) n° 526/2013, et relatif à la certification des technologies de l'information et des communications en matière de cybersécurité (règlement sur la cybersécurité) du 13 septembre 2017,

Vu la communication de la Commission européenne « Un système d'imposition juste et efficace au sein de l'Union européenne pour le marché unique numérique » du 21 septembre 2017,

Considérant que la stratégie de la Commission européenne en faveur du Marché Unique du Numérique vise à favoriser la croissance d'un secteur dans lequel l'Union compte de nombreux atouts ;

Considérant que le potentiel de croissance dans le domaine de l'informatique en nuage pourrait atteindre environ 45 milliards d'euros en 2020 ;

Considérant la nécessité de mettre en œuvre le Règlement général sur la protection des données le 25 mai 2018 ;

Considérant que la protection des données de télécommunication est un complément nécessaire à la protection des données personnelles assurée par le Règlement général sur la protection des données ;

Considérant que la confidentialité des données personnelles doit être protégée, y compris en ce qui concerne les nouveaux acteurs de la télécommunication et ce, dans les différentes phases d'émission, de transit, de réception et de stockage des données ;

Considérant en particulier l'apport du chiffrement dit « de bout en bout » par rapport au chiffrement « de point en point » ;

Considérant qu'il est crucial que l'internaute puisse exprimer, en ce qui concerne les traceurs, un consentement éclairé, libre, spécifique et univoque, tel que défini par le Règlement général sur la protection des données ;

Considérant que la conservation des données sur des terminaux dans la durée doit demeurer une exception circonscrite par un cadre clairement défini et assuré par des mesures proportionnées ;

Considérant qu'il est vain, voire contre-productif, compte tenu des évolutions technologiques actuelles, de contraindre le stockage des données en fonction de considérations nationales ; considérant cependant que la localisation forcée de données peut répondre dans certains cas

dûment justifiés à des questions de sécurité ou de difficulté d'accès aux données ;

Considérant que la libre circulation des données non-personnelles en Europe doit s'accompagner d'un principe de collaboration entre les agences nationales des États membres ;

Considérant qu'il convient de faciliter la possibilité pour l'utilisateur de changer de fournisseur de service en nuage et la portabilité des données personnelles, à l'exclusion des données enrichies par le fournisseur du service ;

Considérant la nécessité de s'assurer de la qualité des produits échangés sur le marché unique du numérique ;

Considérant en particulier que la cybersécurité des produits doit être une priorité et que le degré de certification doit s'adapter à chaque type de produit, mais continuer à s'appuyer sur les standards de certains États membres, dont la France, qui figurent actuellement parmi les plus sécurisés au monde ;

Considérant la nécessité d'encourager tous les États membres à établir une politique publique de cybersécurité ambitieuse ;

Considérant qu'une telle politique ne peut s'appuyer que sur des organes publics ayant les moyens de répondre à des crises répétées mais aussi de diffuser les bonnes pratiques d'hygiène numérique, notamment ;

Considérant qu'une telle politique ne peut être menée actuellement que par les agences nationales, en coordination les unes avec les autres ainsi qu'avec l'ENISA ;

Considérant la nécessité de favoriser l'élaboration, avec les acteurs concernés, d'une doctrine civile d'emploi des technologies de l'information en matière de cybersécurité, dans le respect d'une éthique des entreprises et des principes fondamentaux qui régissent en Europe l'état de droit démocratique ;

Considérant la nécessité d'un système fiscal juste et efficace à l'échelle du marché unique du numérique, condition indispensable à une concurrence loyale entre les entreprises du secteur ;

Considérant le soutien que de nombreux États membres ont apporté à l'initiative française en faveur d'une taxe d'égalisation et l'agenda des travaux mis en place par la Commission européenne à ce sujet le 21 septembre 2017 ;

Considérant, que, selon l'Organisation de coopération et de développement économiques (OCDE), le modèle économique et certains attributs essentiels de l'économie numérique peuvent exacerber les risques d'érosion de la base d'imposition et de transfert des bénéfices ;

Considérant la volonté du Conseil européen de poursuivre la dynamique du chantier européen sur la fiscalité du numérique, en lien avec les travaux pour l'établissement d'une Assiette Commune Consolidée pour l'Impôt sur les Sociétés (ACCIS) ;

1. Salue la poursuite de la stratégie pour un marché unique du numérique par la Commission européenne ;

2. Soutient l'intégration des services de communication par contournement, également appelés *« over the top »*, dans le règlement concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques ;

3. Salue l'interdiction de stocker ou collecter des données sur des terminaux sans le consentement des utilisateurs ;

4. Demande à ce que le consentement de l'utilisateur ne soit pas présumé en amont par le paramétrage automatique du navigateur mais à ce que ce consentement soit recueilli, notamment pour ce qui est des « *cookies* tiers », après une information claire de l'utilisateur ;

5. Estime que l'adaptation de la législation française au Règlement général sur la protection des données doit viser une harmonisation maximale avec nos partenaires européens, afin de favoriser un cadre commun de protection des données personnelles ;

6. Estime que les données relatives au trafic et les données de localisation ne peuvent être conservées par les autorités publiques que de manière proportionnée et uniquement à des fins expresses de sécurité et de défense nationale ;

7. Souhaite garantir aux internautes leur droit d'exprimer le consentement libre, spécifique, éclairé et univoque au traitement des données, sans pour autant compromettre le développement de services numériques à valeur ajoutée dont le modèle économique repose sur l'exploitation des données à des fins publicitaires ;

8. Encourage le Gouvernement à supprimer tout obstacle potentiellement injustifié à la libre circulation des données non-personnelles au sein de l'Union européenne ;

9. Souhaite qu'en complément de cette libre circulation soient mises en place des règles en matière de sécurité et de sûreté des données numériques, qui garantissent la transparence en ce qui concerne la localisation du stockage et du traitement de ces données ainsi que l'assistance mutuelle des autorités nationales pour faciliter l'accès aux données non personnelles stockées sur le territoire de l'Union européenne ;

10. Encourage la création d'un droit à la portabilité des données non personnelles afin de permettre à tout individu ou entreprise de récupérer les données générées par son utilisation d'un service et les transférer facilement auprès d'autres prestataires ;

11. Considère que toute forme de certification des produits, et notamment des objets connectés, doit se faire de manière adaptée à chaque type de produit mais garantir à chaque fois un niveau ambitieux de protection ;

12. Considère à ce titre que la sécurisation des produits doit être fonction de leur exposition au risque et de leur caractère stratégique, pour obéir à une approche proportionnée qui retiendra, selon le degré d'exigence, la solution la plus adéquate selon les niveaux de qualification ;

13. Regrette dans ces conditions la faiblesse du système de certification prévu dans le « paquet » cybersécurité et demande à ce que les autorités nationales en charge de la cybersécurité demeurent, dans tous les États membres, les premières garantes de la protection des citoyens européens dans ce domaine ;

14. Refuse dès lors que l'accroissement du mandat de l'ENISA, l'Agence européenne de cybersécurité, se fasse au détriment de l'action des agences nationales, ce qui pourrait aboutir à une diminution de la cybersécurité dans l'Union européenne ;

15. Se réjouit de l'initiative française en faveur d'une taxe d'égalisation pour les acteurs du numérique ;

16. Souligne que le secteur du numérique est particulièrement soumis aux stratégies non-coopératives aboutissant à l'érosion des bases fiscales et au transfert des bénéfices au sein de l'Union européenne ;

17. Encourage le Gouvernement à appuyer les travaux de la Commission européenne et de la présidence du Conseil à ce sujet, en lien avec les travaux de l'OCDE, en vue d'un schéma de taxation équitable et d'une harmonisation des assiettes fiscales ;

18. Souhaite vivement que, dans le cadre de la proposition de directive sur le droit d'auteur dans le marché unique numérique, les plateformes participent à la juste rémunération des créateurs et à une lutte immédiate et efficace contre le piratage et la contrefaçon ;

19. Soutient les réflexions actuelles de la Commission européenne pour une responsabilité accrue des plateformes dans la lutte contre le contenu illicite en ligne.

AMENDEMENTS EXAMINÉS PAR LA COMMISSION

COMMISSION DES AFFAIRES EUROPÉENNES

6 décembre 2017

PROPOSITION DE RÉSOLUTION EUROPÉENNE SUR LE MARCHÉ UNIQUE DU NUMÉRIQUE (N° 480)

AMENDEMENT

N° 1

présenté par
M. Bothorel, co-rapporteur

ARTICLE UNIQUE

À l'alinéa 18 de la proposition de résolution, remplacer les mots « d'émission, de transit, de réception et de stockage » par les mots « de collecte, de transfert, de traitement, de mise à disposition et de stockage »

EXPOSÉ SOMMAIRE

Cet amendement rédactionnel vise à retenir la terminologie juridique habituellement employée, notamment par la CNIL, pour caractériser le cycle de vie des données.

Cet amendement est adopté.

COMMISSION DES AFFAIRES EUROPÉENNES

6 décembre 2017

PROPOSITION DE RÉSOLUTION EUROPÉENNE SUR LE MARCHÉ UNIQUE DU NUMÉRIQUE (N° 480)

AMENDEMENT

N° 2

présenté par
M. Bothorel, co-rapporteur

ARTICLE UNIQUE

À l'alinéa 23 de la proposition de résolution, remplacer le mot « agences » par le mot « autorités »

EXPOSÉ SOMMAIRE

Cet amendement rédactionnel vise à souligner la diversité des organismes nationaux susceptibles de collaborer en matière de libre circulation des données non-personnelles, au-delà des seules agences nationales.

Cet amendement est adopté.

COMMISSION DES AFFAIRES EUROPÉENNES

6 décembre 2017

PROPOSITION DE RÉSOLUTION EUROPÉENNE SUR LE MARCHÉ UNIQUE DU NUMÉRIQUE (N° 480)

AMENDEMENT

N° 3

présenté par

Mme Karamanli et les commissaires du groupe Nouvelle Gauche

ARTICLE UNIQUE

Au point 5 de la proposition de résolution européenne, après les mots « harmonisation maximale » insérer les mots « par le haut »

EXPOSÉ SOMMAIRE

Cet amendement vise à préciser que s'il y a un besoin évident d'harmonisation, il convient toutefois d'éviter que celle-ci ne conduise à une minoration de la protection des données. L'harmonisation nécessaire doit être une harmonisation par le haut.

Cet amendement est adopté.

COMMISSION DES AFFAIRES EUROPÉENNES

6 décembre 2017

PROPOSITION DE RÉSOLUTION EUROPÉENNE SUR LE MARCHÉ UNIQUE DU NUMÉRIQUE (N° 480)

AMENDEMENT

N° 4

présenté par

M. Bothorel, co-rapporteur

ARTICLE UNIQUE

Au point 6 de la proposition de résolution, supprimer le mot « uniquement »

EXPOSÉ SOMMAIRE

Cet amendement vise à affirmer que, sans aller jusqu'à l'exclusivité, la conservation des données par les autorités publiques doit obéir en premier lieu à des fins expresses de sécurité et de défense nationale.

Cet amendement est adopté..

COMMISSION DES AFFAIRES EUROPÉENNES

6 décembre 2017

PROPOSITION DE RÉSOLUTION EUROPÉENNE SUR LE MARCHÉ UNIQUE DU NUMÉRIQUE (N° 480)

AMENDEMENT

N° 5

présenté par

Mme Karamanli et les commissaires du groupe Nouvelle Gauche

ARTICLE UNIQUE

Au point 7 de la proposition de résolution européenne supprimer les mots « sans pour autant compromettre le développement de services numériques à valeur ajoutée dont le modèle économique repose sur l'exploitation des données à caractère publicitaire »

EXPOSÉ SOMMAIRE

Cet amendement vise à affirmer que le principe du consentement libre des internautes ne doit pas être minoré par le principe de développement des services numériques. La liberté de l'internaute doit être première et pas conditionnée par des considérations liées au marché. C'est pourquoi il serait souhaitable de supprimer l'expression « sans pour autant compromettre le développement des services numériques à valeur ajoutée dont le modèle économique repose sur l'exploitation des données à des fins publicitaires. »

Cet amendement est adopté.

COMMISSION DES AFFAIRES EUROPÉENNES

6 décembre 2017

PROPOSITION DE RÉSOLUTION EUROPÉENNE SUR LE MARCHÉ UNIQUE DU NUMÉRIQUE (N° 480)

AMENDEMENT

N° 6

présenté par

Mme Karamanli et les commissaires du groupe Nouvelle Gauche

ARTICLE UNIQUE

Au point 8 de la proposition de résolution après les mots « au sein de l'Union européenne », insérer les mots « tout en assurant un niveau élevé de protection des données personnelles »

EXPOSÉ SOMMAIRE

Cet amendement vise à affirmer que le principe du consentement libre des internautes et la protection des données personnelles ne doivent pas être minorés par le principe de développement des services numériques. La liberté de l'internaute et la protection de ses données doivent être premières et pas conditionnées par des considérations liées au marché. La libre circulation des données ne doit pas se faire au détriment de la protection des données.

Cet amendement est rejeté.

COMMISSION DES AFFAIRES EUROPÉENNES

6 décembre 2017

PROPOSITION DE RÉSOLUTION EUROPÉENNE SUR LE MARCHÉ UNIQUE DU NUMÉRIQUE (N° 480)

AMENDEMENT

N° 7

présenté par

Mme Karamanli et les commissaires du groupe Nouvelle Gauche

ARTICLE UNIQUE

Après le point 8 de la proposition de résolution insérer un point 8 *bis* :

« Souhaite que le Gouvernement s'engage fortement dans la régulation des plateformes numériques qui, si elles créent de nouveaux modèles économiques, ne doivent pour autant être autorisée à privatiser, au sens d'en prendre le contrôle, un certain nombre de services et de données. »

EXPOSÉ SOMMAIRE

Les plateformes numériques sont à l'origine de nouveaux modèles économiques entre clients et fournisseurs, entre partenaires commerciaux, entre employeurs et travailleurs. Les plateformes peuvent constituer aussi un moyen de « privatisation », au sens d'une prise de contrôle par des grandes entreprises privées, d'un nombre significatif de services et ce hors de toute régulation. Cet amendement vise à souligner ce phénomène et en prévenir les risques.

Cet amendement est rejeté.

COMMISSION DES AFFAIRES EUROPÉENNES

6 décembre 2017

PROPOSITION DE RÉSOLUTION EUROPÉENNE SUR LE MARCHÉ UNIQUE DU NUMÉRIQUE (N° 480)

AMENDEMENT

N° 8

présenté par

Mme Karamanli et les commissaires du groupe Nouvelle Gauche

ARTICLE UNIQUE

Au point 17 de la proposition de résolution ajouter après le terme « assiettes fiscales » l'expression « tout en travaillant à une harmonisation par le haut des taux d'imposition des services numériques ».

EXPOSÉ SOMMAIRE

Cet amendement vise à proposer de travailler à une harmonisation de l'imposition fiscale des services numériques non pas seulement du point de vue des assiettes fiscales mais également des taux d'imposition eux-mêmes.

Cet amendement est adopté.

PROPOSITION DE RÉSOLUTION ADOPTÉE PAR LA COMMISSION

PROPOSITION DE RÉSOLUTION EUROPÉENNE SUR LE MARCHE UNIQUE DU NUMERIQUE

Article unique

L'Assemblée nationale,

Vu l'article 88-4 de la Constitution,

Vu les articles 16 et 114 du TFUE (Traité sur le fonctionnement de l'Union européenne),

Vu la directive n° 95/46/CE du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données,

Vu la directive n° 2002/58/CE 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 ;

Vu le règlement n° 2016/679 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),

Vu le règlement n° 526/2013 du 21 mai 2013 concernant l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) et abrogeant le règlement (CE) n° 460/2004,

Vu la Communication de la Commission européenne « Stratégie pour un marché unique numérique en Europe » du 6 mai 2015,

Vu la Communication de la Commission européenne « Créer une économie européenne fondée sur les données » du 10 janvier 2017,

Vu la proposition de règlement concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques et abrogeant la directive 2002/58/CE (règlement « vie privée et communications électroniques ») du 10 janvier 2017,

Vu la proposition de règlement concernant un cadre applicable à la libre circulation des données à caractère non personnel dans l'Union européenne du 13 septembre 2017,

Vu la proposition de règlement relatif à l'ENISA, Agence de l'Union européenne pour la cybersécurité, et abrogeant le règlement (UE) n° 526/2013, et relatif à la certification des technologies de l'information et des communications en matière de cybersécurité (règlement sur la cybersécurité) du 13 septembre 2017,

Vu la communication de la Commission européenne « Un système d'imposition juste et efficace au sein de l'Union européenne pour le marché unique numérique » du 21 septembre 2017,

Considérant que la stratégie de la Commission européenne en faveur du Marché Unique du Numérique vise à favoriser la croissance d'un secteur dans lequel l'Union compte de nombreux atouts ;

Considérant que le potentiel de croissance dans le domaine de l'informatique en nuage pourrait atteindre environ 45 milliards d'euros en 2020 ;

Considérant la nécessité de mettre en œuvre le Règlement général sur la protection des données le 25 mai 2018 ;

Considérant que la protection des données de télécommunication est un complément nécessaire à la protection des données personnelles assurée par le Règlement général sur la protection des données ;

Considérant que la confidentialité des données personnelles doit être protégée, y compris en ce qui concerne les nouveaux acteurs de la télécommunication et ce, dans les différentes phases de collecte, de transfert, de traitement, de mise à disposition et de stockage des données ;

Considérant en particulier l'apport du chiffrement dit « de bout en bout » par rapport au chiffrement « de point en point » ;

Considérant qu'il est crucial que l'internaute puisse exprimer, en ce qui concerne les traceurs, un consentement éclairé, libre, spécifique et univoque, tel que défini par le Règlement général sur la protection des données ;

Considérant que la conservation des données sur des terminaux dans la durée doit demeurer une exception circonscrite par un cadre clairement défini et assuré par des mesures proportionnées ;

Considérant qu'il est vain, voire contre-productif, compte tenu des évolutions technologiques actuelles, de contraindre le stockage des données en

fonction de considérations nationales ; considérant cependant que la localisation forcée de données peut répondre dans certains cas dûment justifiés à des questions de sécurité ou de difficulté d'accès aux données ;

Considérant que la libre circulation des données non-personnelles en Europe doit s'accompagner d'un principe de collaboration entre les autorités nationales des États membres ;

Considérant qu'il convient de faciliter la possibilité pour l'utilisateur de changer de fournisseur de service en nuage et la portabilité des données personnelles, à l'exclusion des données enrichies par le fournisseur du service ;

Considérant la nécessité de s'assurer de la qualité des produits échangés sur le marché unique du numérique ;

Considérant en particulier que la cybersécurité des produits doit être une priorité et que le degré de certification doit s'adapter à chaque type de produit, mais continuer à s'appuyer sur les standards de certains États membres, dont la France, qui figurent actuellement parmi les plus sécurisés au monde ;

Considérant la nécessité d'encourager tous les États membres à établir une politique publique de cybersécurité ambitieuse ;

Considérant qu'une telle politique ne peut s'appuyer que sur des organes publics ayant les moyens de répondre à des crises répétées mais aussi de diffuser les bonnes pratiques d'hygiène numérique, notamment ;

Considérant qu'une telle politique ne peut être menée actuellement que par les agences nationales, en coordination les unes avec les autres ainsi qu'avec l'ENISA ;

Considérant la nécessité de favoriser l'élaboration, avec les acteurs concernés, d'une doctrine civile d'emploi des technologies de l'information en matière de cybersécurité, dans le respect d'une éthique des entreprises et des principes fondamentaux qui régissent en Europe l'état de droit démocratique ;

Considérant la nécessité d'un système fiscal juste et efficace à l'échelle du marché unique du numérique, condition indispensable à une concurrence loyale entre les entreprises du secteur ;

Considérant le soutien que de nombreux États membres ont apporté à l'initiative française en faveur d'une taxe d'égalisation et l'agenda des travaux mis en place par la Commission européenne à ce sujet le 21 septembre 2017 ;

Considérant, que, selon l'Organisation de coopération et de développement économiques (OCDE), le modèle économique et certains attributs essentiels de

l'économie numérique peuvent exacerber les risques d'érosion de la base d'imposition et de transfert des bénéfices ;

Considérant la volonté du Conseil européen de poursuivre la dynamique du chantier européen sur la fiscalité du numérique, en lien avec les travaux pour l'établissement d'une Assiette Commune Consolidée pour l'Impôt sur les Sociétés (ACCIS) ;

1. Salue la poursuite de la stratégie pour un marché unique du numérique par la Commission européenne ;

2. Soutient l'intégration des services de communication par contournement, également appelés *« over the top »*, dans le règlement concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques ;

3. Salue l'interdiction de stocker ou collecter des données sur des terminaux sans le consentement des utilisateurs ;

4. Demande à ce que le consentement de l'utilisateur ne soit pas présumé en amont par le paramétrage automatique du navigateur mais à ce que ce consentement soit recueilli, notamment pour ce qui est des « *cookies* tiers », après une information claire de l'utilisateur ;

5. Estime que l'adaptation de la législation française au Règlement général sur la protection des données doit viser une harmonisation maximale par le haut avec nos partenaires européens, afin de favoriser un cadre commun de protection des données personnelles ;

6. Estime que les données relatives au trafic et les données de localisation ne peuvent être conservées par les autorités publiques que de manière proportionnée et à des fins expresses de sécurité et de défense nationale ;

7. Souhaite garantir aux internautes leur droit d'exprimer le consentement libre, spécifique, éclairé et univoque au traitement des données ;

8. Encourage le Gouvernement à supprimer tout obstacle potentiellement injustifié à la libre circulation des données non-personnelles au sein de l'Union européenne ;

9. Souhaite qu'en complément de cette libre circulation soient mises en place des règles en matière de sécurité et de sûreté des données numériques, qui garantissent la transparence en ce qui concerne la localisation du stockage et du traitement de ces données ainsi que l'assistance mutuelle des autorités nationales pour faciliter l'accès aux données non personnelles stockées sur le territoire de l'Union européenne ;

10. Encourage la création d'un droit à la portabilité des données non personnelles afin de permettre à tout individu ou entreprise de récupérer les données générées par son utilisation d'un service et les transférer facilement auprès d'autres prestataires ;

11. Considère que toute forme de certification des produits, et notamment des objets connectés, doit se faire de manière adaptée à chaque type de produit mais garantir à chaque fois un niveau ambitieux de protection ;

12. Considère à ce titre que la sécurisation des produits doit être fonction de leur exposition au risque et de leur caractère stratégique, pour obéir à une approche proportionnée qui retiendra, selon le degré d'exigence, la solution la plus adéquate selon les niveaux de qualification ;

13. Regrette dans ces conditions la faiblesse du système de certification prévu dans le « paquet » cybersécurité et demande à ce que les autorités nationales en charge de la cybersécurité demeurent, dans tous les États membres, les premières garantes de la protection des citoyens européens dans ce domaine ;

14. Refuse dès lors que l'accroissement du mandat de l'ENISA, l'Agence européenne de cybersécurité, se fasse au détriment de l'action des agences nationales, ce qui pourrait aboutir à une diminution de la cybersécurité dans l'Union européenne ;

15. Se réjouit de l'initiative française en faveur d'une taxe d'égalisation pour les acteurs du numérique ;

16. Souligne que le secteur du numérique est particulièrement soumis aux stratégies non-coopératives aboutissant à l'érosion des bases fiscales et au transfert des bénéfices au sein de l'Union européenne ;

17. Encourage le Gouvernement à appuyer les travaux de la Commission européenne et de la présidence du Conseil à ce sujet, en lien avec les travaux de l'OCDE, en vue d'un schéma de taxation équitable et d'une harmonisation des assiettes fiscales, tout en visant une harmonisation des taux d'imposition des services numériques ;

18. Souhaite vivement que, dans le cadre de la proposition de directive sur le droit d'auteur dans le marché unique numérique, les plateformes participent à la juste rémunération des créateurs et à une lutte immédiate et efficace contre le piratage et la contrefaçon ;

19. Soutient les réflexions actuelles de la Commission européenne pour une responsabilité accrue des plateformes dans la lutte contre le contenu illicite en ligne.

ANNEXE N° 1 :
LISTE DES PERSONNES AUDITIONNÉES

À Paris :

Syntec numérique

- M. Sébastien Duplan, délégué aux relations institutionnelles.
- Mme Philippine Lefèvre, chargée des relations avec les pouvoirs publics et les acteurs institutionnels de l'écosystème numérique.

Commission Nationale de l'Informatique et des Libertés

- M. Jean Lessi, secrétaire général.
- Mme Tiphaine Havel, conseillère pour les questions institutionnelles et parlementaires.

Conseil National du Numérique

- M. Yann Bonnet, secrétaire général du CNNum.
- M. Jan Krewer, secrétaire général adjoint.
- Mme Judith Herzog, rapporteure.

Quadrature du Net

- M. Arthur Messaud, juriste.

SAP

- Mme Amal Taleb, directrice adjointe des affaires publiques France.
- M. Emmanuel Lempert, directeur des affaires publiques France et Afrique Francophone.

Facebook

- M. Anton'Maria Battesti, *public policy manager*.

Microsoft

- M. Marc Mossé, directeur principal des affaires gouvernementales européennes.
- Mme Corinne Caillaud, directrice des affaires publiques, externes et juridiques.

Qwant

- M. Éric Léandri, co-fondateur et président.
- M. Guillaume Champeau, directeur Ethique et Relations Publiques.
- M. Léonidas Kalogeropoulos, conseil.

Google

- M. Olivier Esper, directeur des relations institutionnelles.
- M. Thibault Guiroy, responsable des relations institutionnelles.

ARCEP

- M. Sébastien Soriano, président.
- Mme Cécile Dubarry, directrice générale.
- Mme Anne Lenfant, directrice Europe et International.

Orange

- M. Pierre Petillault, directeur adjoint aux affaires publiques.
- Mme Claire Chalvidant, directrice des relations institutionnelles.
- M. Laurentino Lavezzi, directeur des affaires publiques.

Cabinet de M. Mounir Mahjoubi, Secrétaire d'État auprès du Premier ministre chargé du Numérique

- M. Grégoire Tirot, directeur de cabinet.

AFNUM

- Mme Maxence Demerlé, déléguée générale.
- Mme Diane Dufoix-Garnier, directrice des Affaires publiques d'IBM.

Croissance Plus

- M. Jean-Baptiste Danet, président.
- M. Nicolas D'Hueppe, vice-président.
- Mme Isabelle D'Halluin, conseillère communication/presse.
- M. Thibault Baranger, chargé des Affaires Publiques et des médias.

Commission Supérieure du Numérique et des Postes

- M. Ludovic Provost, secrétaire général.
- M. André Schwob, personnalité qualifiée.

Hewlett-Packard

- M. David Miguel Ortega Pecina, responsable des affaires publiques Espagne, France et Benelux.

- Mme Catherine Hartog, conseil externe.

Alliance pour la Confiance Numérique

- M. Jean-Pierre Quémard, président.
- M. Yoann Kassianides, directeur général.

Agence nationale de la sécurité des systèmes d'information

- M. Guillaume Poupard, directeur général.
- M. Christian Daviot, chargé de mission stratégie.
- M. Dimitri Petrakis, directeur du bureau des affaires internationales.
- Mme Anne Tricaud, chargée d'affaires publiques.

CISPE / OVH

- M. Alban Schmutz, président de CISPE et vice-président du développement stratégique et des affaires publiques d'OVH.
- M. Stéphane Ducable, membre du conseil de CISPE et directeur de la politique publique d'Amazon Web Services.
- M. Jules-Henri Gavetti, trésorier de CISPE et directeur général d'Ikoula.

Conseil d'État

- M. Timothée Paris, section du rapport et des études.

Chercheur

- M. Stéphane Grumbach, directeur de recherche à l'INRIA.

Spécialiste de la cybersécurité

- M. André Loesekrug-Pietri, fondateur d'A Capital.

À Bruxelles :

Représentation permanente de la France auprès de l'Union européenne

- M. Fabrice Dubreuil, représentant permanent adjoint.
- M. Pascal Rogard, conseiller chargé du numérique, des télécommunications et des postes.

Commission européenne, DG « justice et consommateurs »

- M. Emmanuel Crabit, directeur chargé des droits fondamentaux et de l'État de droit.
- M. Olivier Micol, directeur chargé de la protection des données.

Bureau européen des unions de consommateurs

- Mme Ursula Pachl, directrice générale adjointe.
- M. David Martin, conseiller.

Fédération européenne des éditeurs

- M. Enrico Turrin, directeur général adjoint.

Commission européenne, DG « réseaux de communications, du contenu et des technologies »

- Mme Claire Bury, directeur général adjoint.
- M. Sandor Szalai, *policy officer* au développement et à la coordination et la politique numérique.

Commission européenne, cabinet de M. Andrus Ansip, Vice-président chargé du marché unique numérique

- Mme Laure Chapuis, membre du cabinet.
- M. Jörgen Gren, membre du cabinet.
- Mme Marie Frenay, assistance politique et communication.

Parlement européen

- Mme Françoise Grossetête, membre de la commission de l'industrie, de la recherche et de l'énergie.

Contribution écrite

Canal +