THINK-TANK
DIGITAL
NEW DEAL

DÉFENDRE L'ÉTAT DE DROIT A L'HEURE DES PLATEFORMES

COMBATTRE LES DISCOURS ILLICITES SUR INTERNET ET PROTÉGER LA LIBERTÉ D'EXPRESSION

par Gilles Le Chatelier et Denis Olivennes

juin 2021

Digital New Deal

SOMMAIRE

GILLES LE CHATELIER

Gilles Le Chatelier est professeur associé en droit public (Paris X Nanterre 2003-2005, Lyon II, 2005-2008, Ecole Normale supérieure de Lyon 2008-2020), il préside également le Conseil d'administration de l'IEP de Lyon depuis 2012. Il est également membre du conseil scientifique de l'Actualité Juridique des collectivités territoriales (AJCT) et assure des publications régulières dans de nombreuses revues juridiques spécialisées en droit public.

Après un parcours d'un peu plus de 20 ans au sein de l'administration qui l'a conduit à occuper des responsabilités importantes au sein de l'Etat et des collectivités locales (Conseiller d'Etat, rapporteur adjoint au Conseil constitutionnel, expert auprès de la Commission Européenne,...), Gilles Le Chatelier est devenu avocat en mars 2011 et rejoint à cette occasion le cabinet ADALTYS dont il a pris la présidence en janvier 2020.

DENIS OLIVENNES

Denis Olivennes, ancien haut fonctionnaire, est chef d'entreprise et auteur.

Actuel cogérant du journal Libération. Il fut notamment directeur général de Canal+, président directeur général de la Fnac, du Nouvel Observateur puis de Lagardère Active (Europe 1, Paris Match, Elle, Journal du dimanche ...).

Auteur notamment de *La gratuité, c'est le vol : quand le piratage tue la culture* (2007), *Mortelle transparence* avec Mathias Chichportich (2018) et *Le délicieux malheur français* (2019). Auteur également du *Rapport Olivennes* sur l'offre culturelle et la lutte contre le partage illégal sur internet (2008).

INTRODUCTION

La lutte contre les discours illicites (racistes, antisémites, homophobes, diffamants, injurieux…) sur internet est un défi pour l'ensemble de nos démocraties. La diffusion très large de ces messages constitue un réel danger pour le fonctionnement normal des institutions, sans même parler des manipulations auxquelles les réseaux sociaux ont pu donner lieu lors de plusieurs scrutins récents.

Depuis de nombreuses années, des initiatives ont été prises pour lutter contre ce fléau. Les résultats restent aujourd'hui insuffisants de l'avis unanime. La propagation de ces discours favorise la polarisation de nos sociétés et avive les haines dans un climat malsain. Jusqu'à ce jour, la réaction des hébergeurs, le plus souvent passive, n'a pas permis de lutter efficacement contre ce danger.

Mais en même temps, la volonté de limiter ces contenus pose des questions délicates en matière de respect de la liberté d'expression.

Comme l'a rappelé le Conseil constitutionnel lors de sa décision rendue sur la loi AVIA le 18 juin 2020, en se référant à l'article 11 de la Déclaration des droits de l'Homme et du citoyen garantissant le principe constitutionnel de liberté d'expression : « *en l'état actuel des moyens de communication et eu égard au développement généralisé des services de communication au public en ligne ainsi qu'à l'importance prise par ces services pour la participation à la vie démocratique et l'expression des idées et des opinions,* ***ce droit implique la liberté d'accéder à ces services et de s'y exprimer ».***

Dans ce contexte, les initiatives récentes de plusieurs plateformes censurant des contenus de leur propre initiative ou bloquant des comptes de personnalités politiques, y compris de premier plan, posent nécessairement question.

L'équilibre à trouver est complexe.

Et il doit être recherché à l'échelon européen, plutôt que dans le désordre de réactions nationales dispersées.

Le législateur national est intervenu à plusieurs reprises sur le sujet, avec des fortunes diverses. La censure de la plus grande partie de la Loi Avia du 24 juin 2020 par le Conseil constitutionnel a très largement privé d'effet cette initiative. La reprise par le projet de loi confortant les principes républicains de certaines de ses préoccupations, telles qu'elles figurent dans le texte adopté par l'Assemblée nationale le 16 février 2021, vise à remédier au plan national aux lacunes relevées.

Néanmoins, compte tenu de la puissance des plus grandes plateformes et du caractère éminemment transfrontalier de leurs activités, seule une initiative européenne pourrait être véritablement pertinente.

Comme le relevait la Commission nationale consultative des droits de l'Homme (CNCDH) dans son avis du 9 juillet 2019 sur la proposition de loi AVIA, « la CNCDH regrette aussi l'absence de coordination des Etats, tant au niveau de l'Union européenne qu'au niveau international ».

De la même manière, le Conseil d'Etat dans son avis sur le même texte, émis le 16 mai 2019 indiquait que *« seule l'adoption de nouvelles dispositions par l'Union européenne donnerait un fondement commun et une efficacité considérablement accrue à une lutte que les valeurs inscrites dans les Traités imposent de conduire en même temps que le marché se développe ».*

Or, le cadre juridique en vigueur aujourd'hui apparaît largement lacunaire (1). Une proposition de règlement européen vient d'être déposée par la Commission, le « Digital Service Act », dont il faut saluer le mérite car elle va dans la bonne direction sur un certain nombre de points (2). Toutefois, même au stade de cette proposition, qui doit encore être avalisée par le Parlement européen et le Conseil, certaines lacunes demeurent qui méritent d'être comblées par des propositions complémentaires (3).

1. UN CADRE JURIDIQUE EUROPÉEN ACTUEL INSUFFISANT

1.1 LA DIRECTIVE DE 2000

Les dispositions applicables en ce domaine résultent d'un texte désormais un peu ancien, **la directive n°2000/31/CE 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.

Comme l'indique son intitulé même, ce texte porte principalement sur le commerce électronique et met en œuvre les moyens de lever les éventuels obstacles au développement de celui-ci dans l'espace européen. La base juridique de ce texte résulte des articles du Traité relatifs au marché intérieur.

Néanmoins, plusieurs dispositions de ce texte traitent de la question des contenus, en particulier aux articles 12 à 15 de ce texte.

Comme l'indique le § 40 des motifs de la directive, « la présente directive doit constituer la base adéquate pour l'élaboration de mécanismes rapides et fiables permettant de retirer les informations illicites et de rendre l'accès à celles-ci impossible ».

Les sujets des contenus illicites et des moyens de les contrôler figurent aux articles 12 à 15 de la directive.

L'article 14 de la directive porte sur les obligations des hébergeurs. Elle pose **le principe de l'irresponsabilité de ces derniers quant aux informations stockées**. Toutefois, leur irresponsabilité est soumise à la double condition que :

- *« le prestataire n'ait pas effectivement connaissance de l'activité ou de l'information illicites et, en ce qui concerne une demande en dommages et intérêts, n'ait pas connaissance des faits ou de circonstances selon lesquels l'activité ou l'information illicite est apparente ;*
- *Le prestataire, dès le moment où il a de telles connaissances, agisse promptement pour retirer les informations ou rendre l'accès à celle-ci impossible ».*

Ce dispositif est minimal est laisse une certaine latitude aux Etats membres, l'article 14.3 de la directive permettant à une juridiction ou à une autorité administrative d'un Etat membre d'exiger de l'hébergeur qu'il mette un terme à la présence de contenus illicites ou qu'il prévienne cette situation.

De même, les Etats membres sont libres d'instaurer des procédures régissant le retrait des contenus illicites et les actions pour en rendre l'accès impossible. Le § 46 des motifs de la directive précise cependant que ces opérations doivent s'effectuer *« dans le respect du principe de liberté d'expression et des procédures établies à cet effet au niveau national ».*

L'article 15 de ce texte pose le deuxième principe majeur sur ces questions : **l'absence de toute obligation générale pour les hébergeurs en matière de surveillance.**

Comme l'indique l'article 15.1 de la directive :

> *« Les Etats membres ne doivent pas imposer aux prestataires…une obligation générale de surveiller les informations qu'ils transmettent ou stockent, ou une obligation générale de rechercher activement des faits ou des circonstances révélant des activités illicites ».*

L'article 15.2 prévoit cependant que ces dispositions ne concernent pas les obligations de surveillance applicables à un « cas spécifique ». Les Etats membres peuvent ainsi prévoir des systèmes dans lesquels les hébergeurs seraient tenus de signaler les contenus illicites dont ils auraient connaissance ainsi que de répondre aux sollicitations des autorités leur demandant d'identifier les destinataires de leurs services qui diffuseraient de tels contenus.

La CJUE a ainsi jugé que ces dispositions ne faisaient pas obstacle à ce qu'une juridiction d'un Etat membre enjoigne à un hébergeur de supprimer les informations qu'il stocke et dont le contenu est identique à celui d'une information déclarée illicite précédemment ou de bloquer l'accès à celles-ci, quel que soit l'auteur de la demande de stockage de ces informations (CJUE 3 octobre 2019 Glawischnig-Piesczek n°C-18 /18).

1.2 UN TEXTE DATÉ

Le texte de la directive, antérieur au développement phénoménal des plateformes numériques, est à l'évidence inadapté à la prise en compte des enjeux rappelés précédemment. Comme l'écrit le Conseil d'Etat dans son avis du 16 mai 2019 sur la proposition de loi AVIA *« le dispositif de la directive e-commerce est antérieur de plusieurs années à la création des réseaux sociaux et l'ampleur du déferlement de contenus odieux appelle une action urgente de défense des personnes ».*

Le Conseil européen partage le même constat en indiquant que *« l'extension et la diversité des nouveaux modèles d'entreprise et services numériques ont considérablement évolué avec le temps et que certains services ont créé de nouveaux défis que le cadre règlementaire existant ne couvre pas toujours. » (« Façonner l'avenir numérique de l'Europe – conclusions du Conseil 9 juin 2020 »).*

Surtout l'affirmation du double principe de responsabilité limitée de l'hébergeur et d'interdiction d'obligation de surveillance générale aboutit à des situations où, dans la pratique, des contenus illicites peuvent demeurer en ligne pendant de longues durées au risque de provoquer de graves dommages.

Pour répondre à ces insuffisances, les institutions européennes ont développé des codes de conduite afin d'inciter en particulier les hébergeurs à mettre en œuvre les moyens nécessaires pour lutter contre la présence de contenus illicites, comme le prévoyaient d'ailleurs les dispositions de l'article 16 de la directive du 8 juin 2000.

Ainsi, a été conclu, à l'initiative de la Commission européenne, le 31 mai 2016, un « code de conduite pour contrer le discours de haine illégal en ligne » auquel ont souscrit Facebook, Twitter, YouTube et Microsoft, rejoints en 2018 par Google +, Instagram, Snapchat et Dailymotion.

De même, la Commission a édicté le 1er mars 2018 des recommandations sur les mesures destinées à lutter, de manière efficace, contre les contenus illicites en ligne (C(2018) 1177 final).

Toutefois, ces initiatives, même si elles peuvent être intéressantes, relèvent d'une approche

de « soft law » par nature peu contraignante pour les opérateurs. Le degré de protection qui en résulte est ainsi nécessairement limité, en particulier pour les personnes susceptibles d'être affectées par des discours de haine.

Ainsi, les textes actuels ne présentent de garanties suffisantes ni pour la lutte contre les discours de haine ni pour la liberté d'expression.

2. LA PROPOSITION DE LA COMMISSION D'UN RÈGLEMENT EUROPÉEN SUR CES QUESTIONS – LE « DIGITAL SERVICE ACT » (DSA)

Ce constat d'insuffisance explique largement la proposition faite par la Commission Européenne le 15 décembre 2020 d'un nouveau Règlement européen relatif à un marché intérieur des services (législation sur les services numériques) et modifiant la directive 2000/31/CE, dite « Digital Service Act » (DSA) dont il faut saluer l'heureuse initiative.

Ce texte contient un certain nombre d'avancées significatives qui méritent d'être soulignées et soutenues.

La proposition de Règlement abroge les articles 12 à 15 de la directive du 8 juin 2020 pour y substituer un nouveau régime. Toutefois, il en conserve les principes fondamentaux comme nous le verrons ultérieurement.

Le texte ajoute des obligations supplémentaires ayant pour effet de modifier profondément le régime aujourd'hui en vigueur en vue d'en accroître l'efficacité.

Il est organisé en trois parties : la définition d'un certain nombre d'obligations générales applicables à tous les acteurs (2.1.), une gradation des obligations en fonction de la taille des opérateurs (2.2.) et le renforcement des dispositifs nationaux de contrôle en lien avec les institutions communautaires (2.3.).

2.1 DES OBLIGATIONS GÉNÉRALES RENFORCÉES

La proposition de Règlement comporte de nouvelles règles, applicables à tous les opérateurs, de nature à renforcer la lutte contre les contenus illicites, ainsi qu'à permettre un meilleur contrôle des opérations de retrait de contenus sur internet.

Comme l'indique le § 34 des motifs du projet de Règlement : *« Afin d'atteindre les objectifs du présent règlement …il est nécessaire d'établir un ensemble clair et équilibré d'obligations harmonisées de diligence pour les fournisseurs de services intermédiaires. Ces obligations devraient notamment viser à garantir différents objectifs de politique publique, comme celui d'assurer la sécurité et la confiance des bénéficiaires du service, y compris les mineurs et les utilisateurs vulnérables, protéger les droits fondamentaux pertinents inscrits dans la Charte, assurer une véritable responsabilisation de ces fournisseurs et donner les moyens d'agir aux bénéficiaires et autres parties concernées, tout en facilitant la nécessaire surveillance par les autorités compétentes. »*

Le règlement donne également **une définition du contenu illicite** (article 2 g) comme *« toute information qui en soi ou de par sa référence à une activité…n'est pas conforme au droit de l'Union ou au droit d'un Etat membre, quel qu'en soit l'objet précis ou la nature précise ».*

Le § 12 des motifs précise que *« ce concept doit être compris comme se référant à des informations, quelle que soit leur forme, qui, en vertu du droit applicable, sont soit elles-mêmes illicites, comme les discours de haine illégaux ou les contenus à caractère terroriste*

et les contenus discriminatoires illégaux, soit se rapportent à des activités illégales, comme le partage d'images représentant des abus sexuels commis sur des enfants, le partage illégal d'images privées sans consentement, le harcèlement en ligne, la vente de produits non conformes ou contrefaits, l'utilisation non autorisée de matériel protégé par le droit d'auteur ou les activités impliquant des infractions à la loi sur la protection des consommateurs ».

Les modifications proposées sont ainsi de plusieurs ordres.

- **Injonctions** (articles 8 et 9) : la première série d'injonctions prévues par cet article concernent les contenus illicites. Le texte impose au fournisseur de services d'informer « dans les meilleurs délais » l'autorité qui l'a saisi de la suite qui lui a été donnée. L'autorité qui adresse l'injonction doit motiver sa demande, ainsi que donner des informations permettant d'identifier l'émetteur du contenu (adresses URL exactes ou « informations complémentaires »). Elle doit également donner des informations sur les voies de recours possibles contre l'injonction. Un dispositif similaire est prévu pour les injonctions que peuvent émettre les autorités nationales aux hébergeurs leur demandant de fournir certaines informations.
- **Point de contact unique** (article 10) : les fournisseurs de services intermédiaires doivent établir un tel point de contact vis-à-vis des autorités nationales ou européennes pour faciliter les relations avec elles et les rendre plus fluides.
- **Représentants légaux** (article 11) : cette disposition impose aux fournisseurs qui n'ont pas d'établissement au sein de l'Union européenne de désigner une personne morale ou physique pour les représenter légalement. Ces représentants doivent être en mesure de répondre auprès des autorités nationales et communautaires de toutes les questions relatives à l'exécution des obligations figurant dans le règlement. Ils doivent disposer à cet effet des « pouvoirs nécessaires » pour coopérer et peuvent *« être tenus responsables du non-respect des obligations ».*
- **Transparence en matière d'opérations de modération** (article 13) : les fournisseurs de services doivent établir périodiquement des rapports sur les éventuelles opérations de modération auxquelles ils se sont livrés, que ce soit sur injonction ou de leur propre initiative, ou en réponse à des réclamations.

2.2 DES OBLIGATIONS D'INTENSITÉ CROISSANTE SELON LA TAILLE DE L'OPÉRATEUR

Comme l'indique le § 35 de la motivation du projet de règlement, *« il est important que les obligations de diligence soient adaptées au type et à la nature du service intermédiaire concerné ».*

Cette différenciation des obligations en fonction de la taille des opérateurs est une des novations majeures de la proposition. Elle va effectivement dans la bonne direction en modulant l'intensité des obligations selon la taille de l'opérateur auquel elles s'appliquent.

La proposition de règlement impose ainsi des obligations croissantes aux fournisseurs de services d'hébergement, aux plateformes en ligne (PFL) et aux très grandes plateformes en ligne (TGPFL).

Dès lors, le projet de règlement procède à la définition de ces trois séries d'opérateurs.

En premier lieu, il définit **les fournisseurs de services d'hébergement** comme ceux dont l'activité consiste *« à stocker des informations fournies par un bénéficiaire du service à la demande de ce dernier ».*

En second lieu, l'article 2 h) du projet définit **les plateformes en ligne** comme *« tout fournisseur de service d'hébergement qui, à la demande d'un bénéficiaire du service, stocke et* ***diffuse au public des informations****, à moins que cette activité ne soit une caractéristique mineure et purement accessoire d'un autre service qui, pour des raisons objectives et techniques, ne peut être utilisée sans cet autre service, et pour autant que l'intégration de cette caractéristique à l'autre service ne soit pas un moyen de contourner l'applicabilité du présent règlement ».*

Le § 13 des motifs de la proposition permet de distinguer plus clairement les plateformes en ligne qui constituent ainsi une sous-catégorie des fournisseurs de services d'hébergement :

> *« les plateformes en ligne, telles que les réseaux sociaux ou les places de marché en ligne, devraient être définies comme des fournisseurs de services d'hébergement qui non seulement stockent les informations fournies par les bénéficiaires du service à leur demande, mais qui diffusent également ces informations au public, toujours à leur demande. Toutefois, afin d'éviter d'imposer des obligations trop étendues, les fournisseurs de services d'hébergement ne devraient pas être considérés comme des plateformes en ligne lorsque la diffusion au public n'est qu'une caractéristique mineure et purement accessoire d'un autre service et que cette caractéristique ne peut, pour des raisons techniques objectives, être utilisée sans cet autre service principal, l'intégration de cette caractéristique n'étant pas un moyen de se soustraire à l'applicabilité des règles du présent règlement relatives aux plateformes en ligne. Par exemple, la section «commentaires» d'un journal en ligne pourrait constituer une telle caractéristique, lorsqu'il est clair qu'elle est accessoire au service principal représenté par la publication d'actualités sous la responsabilité éditoriale de l'éditeur ».*

Enfin, en dernier lieu, l'article 25 du projet de règlement définit **les très grandes plateformes en ligne** comme celles *« fournissant leurs services à un nombre mensuel moyen de bénéficiaires actifs du service au sein de l'Union égal ou supérieur à 45 millions ».*

Comme l'indique la Commission, *« étant donné le rôle important que jouent les très grandes plateformes en ligne, en raison de leur audience, exprimée notamment en nombre de bénéficiaires du service, dans la facilitation du débat public, des transactions économiques, et de la diffusion d'informations, d'opinions et d'idées, et compte tenu de l'influence qu'elles exercent sur la manière dont les bénéficiaires obtiennent et communiquent des informations en ligne, il est nécessaire d'imposer à ces plateformes des obligations spécifiques qui viennent s'ajouter aux obligations applicables à toutes les plateformes en ligne ».*

Ainsi, le projet de texte prévoit des obligations applicables aux services d'hébergement, aux PFL et d'autres supplémentaires applicables aux seules TGPFL.

A. LES OBLIGATIONS APPLICABLES À TOUS LES SERVICES D'HÉBERGEMENT

Deux nouveaux dispositifs sont ici prévus qui s'imposent à l'ensemble des hébergeurs de contenus :

- **Mécanismes de notification** (article 14) : les fournisseurs de services doivent prévoir des mécanismes standardisés et simples permettant à toute personne de leur

signaler des contenus considérés comme illicites. Ces notifications sont considérées comme des éléments portant à la connaissance de l'hébergeur cette situation et le contraignant à agir sous peine d'être susceptible d'engager sa responsabilité en cas d'inaction. L'hébergeur doit accuser réception de cette notification et indiquer à la personne qui l'a saisi des suites qui lui ont été données.

- **Motivation des décisions de retrait de contenu ou d'accès** (article 15) : l'hébergeur doit informer au plus tard au moment du retrait ou du blocage la personne concernée de cette décision. Il doit également lui indiquer les raisons de cette décision, l'utilisation éventuelle de « moyens automatisés » pour prendre la décision et les références juridiques expliquant pour quelle raison il considère le contenu comme illicite. Il doit également lui communiquer les voies de recours à sa disposition pour éventuellement contester cette décision.

B. LES OBLIGATIONS SUPPLÉMENTAIRES APPLICABLES AUX PLATEFORMES EN LIGNE

En sus des obligations qui précèdent, le projet de règlement impose des règles particulières.

- **Système interne de traitement des réclamations** (article 17) : les PFL doivent mettre en place des dispositifs internes des réclamations contre les décisions prises par elles s'agissant de contenus illicites ou « incompatibles avec leurs conditions générales » et ayant pour effet le retrait d'un contenu ou un blocage d'accès, la suspension ou la résiliation de la fourniture du service, la suspension ou la résiliation du compte du bénéficiaire. Les PFL doivent traiter ces réclamations « en temps opportun, de manière diligente et objective ». Les bénéficiaires de services de PFL subissant une des décisions mentionnées plus haut doivent pouvoir s'adresser à un organe de règlement extra-judiciaire des litiges certifié par les autorités nationales (article 18).

- **Signaleurs de confiance** (article 19) : il appartient aux autorités nationales de doter certaines entités de cette qualification dont les notifications telles que prévues à l'article 14 du projet de règlement devront faire l'objet d'un traitement prioritaire par la PFL « et dans les meilleurs délais ». Pour obtenir une telle qualification, l'organisme considéré doit disposer d'une expertise particulière dans l'identification des contenus illicites et représenter des intérêts collectifs distincts de ceux de la PFL .

- **Mesures de lutte et de protection contre les utilisations abusives** (article 20) : ce nouveau dispositif vise à lutter contre la répétition d'infractions par les mêmes utilisateurs. A cet effet, les PFL peuvent suspendre, après les avoir avertis, les bénéficiaires de services « qui fournissent fréquemment des contenus manifestement illicites ». Un même dispositif est prévu pour les personnes abusant des dispositifs de notification (article 14) ou de réclamation (article 17). Les PFL jugent du caractère abusif de ce comportement au regard du nombre d'abus recensés, de la gravité de leurs conséquences et de l'intention de la personne en cause.

- **Notification de soupçons d'infraction pénale** (article 21) : lorsqu'une PFL a connaissance d'informations laissant soupçonner « qu'une infraction pénale grave impliquant une menace pour la vie ou la sécurité des personnes a été commise, est commise ou est susceptible de l'être » elle en informe « promptement » les services répressifs compétents de l'Etat membre.

C. LES OBLIGATIONS IMPOSÉES AUX TRÈS GRANDES PLATEFORMES EN LIGNE

Des dispositifs supplémentaires s'imposent enfin aux TGPFL.

- **Évaluation des risques systémiques** (article 26) : les TGPFL doivent analyser au moins une fois par an, tout risque systémique trouvant son origine dans le fonctionnement et l'utilisation de leurs services au sein de l'Union.

Les trois risques systémiques suivant sont identifiés :

- La diffusion de contenus illicites, en particulier la diffusion de matériel pédopornographique et les discours de haine ;
- La remise en cause des droits fondamentaux, y compris la liberté d'expression et d'information, le droit à la vie privée, le droit à la non-discrimination et les droits de l'enfant. Le §57 des motifs du projet cite à ce titre la conception de systèmes algorithmiques susceptibles de produire ces effets néfastes ;
- Les manipulations intentionnelles de leurs services avec des effets négatifs prévisibles sur la santé, le discours civique, les processus électoraux, la sécurité publique et la protection des mineurs ;

Dans cette évaluation des risques, les TGPFL doivent prendre en compte leurs systèmes de modération, ainsi que leurs systèmes de recommandation, de sélection et d'affichages des contenus.

Les TGPFL doivent en conséquence prendre des mesures d'atténuation de ces risques systémiques (article 27) : adaptation des systèmes de modération, renforcement des procédures internes de surveillance des activités, mise en place de coopérations renforcées avec les signaleurs de confiance.

- **Organisation d'audits indépendants** (article 28) : chaque année, les TGPFL doivent organiser à leurs frais un audit indépendant pour vérifier le respect de leurs obligations au titre du projet de règlement. Les audits réalisés par des organismes qualifiés indépendants des TGPFL émettent des recommandations à l'issue de leurs investigations auxquelles les TGPFL doivent répondre par des mesures de mise en œuvre dans un délai d'un mois.
- **Systèmes de recommandation** (article 29) : les TGPFL qui utilisent de tels systèmes doivent établir « de manière claire, accessible et aisément compréhensibles » les principaux paramètres de ces systèmes, ainsi que les options dont disposent les bénéficiaires de leurs services pour pouvoir les modifier ou les adapter.
- **Accès et contrôle des données** (article 31) : les TGPFL fournissent aux Etats membres ou à la Commission l'accès aux données nécessaires pour contrôler et évaluer leur respect des obligations ainsi fixées. Des chercheurs agréés peuvent être désignés par les autorités publiques pour procéder à l'analyse des risques systémiques visés à l'article 26 du présent projet de règlement.
- **Responsables de la conformité** (article 32) : les TGPFL doivent désigner une ou plusieurs personnes chargées de contrôler le respect par elles du présent règlement. Elles doivent assurer qu'ils puissent accomplir leurs fonctions en toute indépendance.

2.3 LES DISPOSITIFS NATIONAUX ET EUROPÉENS DE CONTRÔLE

Le projet de règlement contient de nombreuses dispositions ayant trait aux modes de contrôle par les autorités nationales et européennes du respect de ces obligations par les hébergeurs. Ce point constitue une nouveauté importante, la directive du 8 juin 2000 ne comportant aucune disposition portant sur ces questions.

Plusieurs dispositifs sont ainsi prévus pour contraindre les Etats membres à mettre en place les moyens nécessaires pour s'assurer du respect des règles figurant dans le présent projet de règlement. Est également réglée la question de l'Etat membre responsable de ce contrôle compte tenu des implantations de l'hébergeur. De même, des pouvoirs accrus sont proposés aux instances européennes pour jouer un plus grand rôle dans la gestion de ces questions.

- **Mise en place de coordinateurs nationaux** (article 38) : chaque Etat membre doit désigner une autorité nationale comme coordinateur pour les services numériques, responsable de l'application du présent règlement sur tout le territoire de l'Etat membre. Il chapeaute l'activité de toutes les instances nationales susceptibles d'intervenir pour l'application des règles proposées.

  Il dispose de pouvoirs d'enquête étendus (article 41), notamment celui de procéder à des inspections sur place. Il peut également ordonner la cessation des infractions constatées et imposer des mesures correctives et infliger des amendes ou des astreintes.

  Les coordinateurs nationaux peuvent mener des enquêtes conjointes (article 46) pour les hébergeurs agissant dans plusieurs Etats membres. Ils peuvent également saisir la Commission pour diligenter une enquête si les manquements résultent de l'activité des TGPFL. Les coordinateurs nationaux sont regroupés dans un Comité européen des services numériques qui doit les assister dans l'accomplissement de leurs missions (article 47).

- **Compétence** (article 40) : l'Etat membre dans lequel l'hébergeur a son établissement principal est celui compétent au titre du présent règlement. Si l'hébergeur ne dispose pas d'établissement au sein de l'UE, c'est l'Etat membre où est établi son représentant légal qui est compétent. De manière plus novatrice, s'il n'est satisfait à aucune des deux conditions précédentes, l'ensemble des Etats membres de l'UE peuvent agir contre l'hébergeur qui méconnaîtrait ses obligations. Cette règle permet ainsi d'introduire une logique de compétence d'intervention en fonction du lieu de destination du service, et pas nécessairement en fonction du siège de l'hébergeur.

- **Sanctions** (article 42) : les Etats membres doivent prévoir des mécanismes de sanction à l'encontre des hébergeurs qui ne respecteraient pas leurs obligations. Celles-ci doivent être « effectives, proportionnées et dissuasives ». Elles ne doivent pas dépasser 6 % des revenus ou du chiffre d'affaires annuel (5% pour les astreintes).

- **Mesures particulières de contrôle des TGPFL** : le projet de règlement européen prévoit des dispositifs particuliers de contrôle sur les TGPFL dans lesquels la Commission européenne joue un rôle important dans la conduite des investigations (articles 51 et suivants). Cette mission peut aller jusqu'à la condamnation à des sanctions pouvant également aller jusqu'à 6 % du chiffre d'affaires total réalisé.

La proposition de règlement renforce considérablement les obligations pesant sur les hébergeurs ainsi que les systèmes de contrôle et de sanction auxquels ces derniers sont soumis. Toutefois, malgré ces avancées qui doivent certainement être soutenues, plusieurs questions restent, à ce stade, non réglées par la proposition et nécessitent certainement des avancées plus significatives.

3. UNE PROPOSITION QUI DOIT ENCORE ÊTRE COMPLÉTÉE

Malgré des avancées significatives, la proposition de règlement européen doit être amendée sur plusieurs points importants.

En effet, il n'est pas certain que le texte réponde à la « feuille de route » esquissée par le Conseil dans ses conclusions du 9 juin 2020 appelant à *« la nécessité d'établir des règles claires, harmonisées et fondées sur des éléments probants en matière de responsabilités et d'obligation de rendre des comptes pour les services numériques, qui garantiraient aux intermédiaires de l'internet un niveau adéquat de sécurité juridique».*

3.1 LE RÉGIME DE RESPONSABILITÉ

Comme indiqué précédemment, **la proposition de règlement ne remet pas en cause le principe de responsabilité limitée dont bénéficient les hébergeurs.**

L'article 5 du projet de règlement rappelle ainsi le principe selon lequel « le fournisseur n'est pas responsable des informations stockées à la demande d'un bénéficiaire ». Sa responsabilité peut être mise en cause si l'hébergeur a effectivement connaissance de l'activité ou du contenu illicite, et, dès lors qu'il a connaissance d'une telle situation, qu'il n'a pas agi « promptement » pour retirer le contenu illicite ou rendre l'accès à celui-ci impossible.

Il s'agit ici en réalité de la reprise pure et simple des dispositions qui figurent aujourd'hui à l'article 14 de la directive du 8 juin 2000 que le projet présent de règlement ne modifie pas fondamentalement.

La Commission justifie cette position en indiquant que *« la sécurité juridique offerte par le cadre horizontal d'exemptions conditionnelles de responsabilité pour les fournisseurs de services intermédiaires, établi par la directive 2000/31/CE, a permis l'émergence et le développement de nombreux services nouveaux dans l'ensemble du marché intérieur.* ***Il convient, dès lors, de conserver ce cadre ».***

La seule avancée effective est le système de notifications prévu à l'article 14 qui permet de formaliser une série de situations dans lesquelles l'hébergeur ne peut dégager sa responsabilité, ce dernier devant alors être considéré comme ayant eu connaissance de la présence de contenus illégaux sur sa plateforme dès lors qu'il a reçu une telle notification.

Pour le reste, le principe de responsabilité limitée des hébergeurs demeure.

Cette situation ne paraît pas pouvoir être maintenue en l'état. Dans les faits, il apparait de plus en plus clairement que, loin d'accueillir passivement des contributions, les hébergeurs procèdent à des choix éditoriaux : par la mise en avant et par la recommandation de contenus ou par la censure qu'ils exercent sur certains d'entre eux selon des règles de modération qui leur sont propres.

Plusieurs voies d'amélioration sont possibles à ce titre.

La première doit porter sur la question **du « fait déclencheur »** pour provoquer l'intervention de l'hébergeur.

Plusieurs dispositions sont prévues dans le projet de règlement :

- Le dispositif de notifications (article 14) à l'initiative des personnes physiques et morales qui signalent à l'hébergeur un contenu illicite ;
- Les signaleurs de confiance (article 19) dont les notifications de contenus illicite « donnent lieu à des décisions de manière prioritaire et dans les meilleurs délais » ;
- La mise en place de responsables de la conformité (article 32) dans les seules TGPFL, chargés de contrôler le respect par elle de ses obligations
- Les pouvoirs reconnus aux coordinateurs en ligne « d'ordonner la cessation des infractions et d'imposer les mesures correctives nécessaires pour faire cesser l'infraction » (article 41.2).

Ces nouvelles dispositions doivent être effectivement soutenues en vue de leur adoption dans le règlement définitif.

La seconde question porte sur **le délai de réaction** dont dispose l'hébergeur en présence d'un contenu qui lui est signalé comme illicite.

Dans la proposition de la Commission européenne, l'obligation de réagir « promptement » - rédaction maintenue de la directive du 8 juin 2000- reste toujours aussi floue quant à la question de l'appréciation du délai de réaction de l'hébergeur, ce point conditionnant la mise en cause de sa responsabilité éventuelle. Or, à défaut de précision plus claire sur le délai dont dispose l'hébergeur pour réagir, le risque est grand que le contenu illicite en cause puisse rester en ligne sur une longue durée. La voie est cependant étroite sur ces questions. Comme on l'a rappelé en effet, la loi AVIA avait achoppé sur ce point en imposant, selon le juge constitutionnel, des délais trop courts pour réagir (1 heure pour les contenus à caractère terroriste ou pédopornographique, 24 h pour une liste très importante de contenus illicites), le manquement à ces obligations étant assorti potentiellement de lourdes peines (1 an d'emprisonnement et 250 K€ d'amende).

De même, le Conseil constitutionnel avait également sanctionné dans la loi AVIA le fait qu'aucune clause d'exonération claire de l'hébergeur n'était prévue, que la liste des infractions rendait le travail d'examen particulièrement délicat et que la sanction pénale était particulièrement lourde.[1]

Plusieurs propositions pourraient cependant être faites pour améliorer la proposition de la Commission sans risquer à première vue une censure par le juge constitutionnel français[2] :

- La première pourrait consister à prévoir un délai très court (24 h) pour réagir à une saisine par un signaleur de confiance. Cette obligation ne pourrait concerner que les Très Grandes Plateformes en Ligne (et pas les autres hébergeurs). Il convient

[1] *L'ensemble de ces éléments explique la raison pour laquelle le CNCDH avait donné un avis très négatif à la proposition de loi AVIA en estimant que le dispositif proposé risquait de conduire les hébergeurs à des attitudes si prudentes que ce serait la liberté d'expression qui serait au final menacée*

[2] *On rappellera à ce titre que selon la jurisprudence du Conseil constitutionnel, les règles de droit européen restent soumises dans la hiérarchie des normes aux règles figurant dans la Constitution (CC décision du 19 novembre 2004)*

de noter que le code de conduite conclu en mai 2016 assignait déjà un tel objectif aux TGPFL signataires de l'accord[3] ;

- Le délai pourrait être ramené à une période plus courte pour certaines infractions dûment énumérées et correspondant à des délits particulièrement graves (pédopornographie, incitation au terrorisme…) ;
- De la même manière, les délais d'intervention ne devraient pas être identiques selon l'audience du bénéficiaire considéré ; la présence sur une longue durée d'un contenu qui pourra être vu par des milliers (millions) d'internautes n'a pas les mêmes conséquences que la même infraction qui ne concernerait que quelques personnes.
- Les sanctions pour le non-respect de ces délais d'examen pourraient être également modulées en fonction de la nature du contenu illicite considéré et des clauses d'exonération précises pour l'hébergeur définies par le futur règlement ;
- Les hébergeurs devraient déterminer des chartes internes de lutte contre les contenus illicites (ceux-ci étant exclusivement définis par la loi nationale ou européenne et non par des règles internes aux plateformes) qui seraient juridiquement contraignantes vis-à-vis des utilisateurs de leurs services et dont la méconnaissance serait susceptible d'engager leur responsabilité. Figureraient dans cette charte des éléments relatifs au fonctionnement de la modération, à l'ordonnancement des contenus et aux paramètres des algorithmes et à leur évolution ; le contrôle du respect de ces engagements serait bien évidemment assuré par la puissance publique, toute infraction à ces obligations étant susceptible de mettre en cause la responsabilité des hébergeurs ;
- L'obligation d'un certain devoir de surveillance des contenus (voir infra) qui ne remette pas en cause le principe de l'absence d'obligation générale de surveillance mais qui s'inscrit dans le cadre prévu par l'article 15 de la directive n°2000/31/CE du 8 juin 2000.

Toutefois, la question de la sanction des hébergeurs dans l'hypothèse où ceux-ci ne seraient pas assez diligents pour supprimer les contenus illicites reste entièrement posée. A l'heure actuelle, les sanctions prononcées à ce titre restent symboliques (cf Rapport CNCDH du 10 juillet 2015 sur la lutte contre les discours de haine sur internet). Pour autant, des sanctions trop lourdes ne doivent pas apparaître « disproportionnées » au risque d'une attitude favorisant des phénomènes d'auto-censure de la part des plateforme, préjudiciables à terme à l'exercice de la liberté d'expression.

3.2 L'ABSENCE D'OBLIGATION DE SURVEILLANCE GÉNÉRALE

Une nouvelle fois le projet de règlement européen ne modifie en rien sur ce point le dispositif issu de la directive du 8 juin 2000.

L'article 7 prévoit ainsi que : *« les fournisseurs de services intermédiaires ne sont soumis à aucune obligation générale de surveiller les informations qu'ils transmettent ou stockent, ou de rechercher activement des faits ou des circonstances révélant des activités illicites ».*

[3] *« Les entreprises des technologies de l'information signataires de ce code de conduite s'engagent à continuer la lutte contre les discours de haine illégaux en ligne. Elles poursuivront notamment la mise au point de procédures internes et assureront la formation du personnel pour que la majorité des signalements valides puissent être examinés en moins de 24 heures et, s'il y a lieu, pour retirer les contenus visés et bloquer l'accès. »*

C'est la reprise quasiment à l'identique des dispositions de l'article 13 de la directive du 8 juin 2000.

Pourtant sans imposer cette obligation de surveillance générale dont on peut comprendre ce qu'elle pourrait avoir de délicat au regard du respect des libertés fondamentales en général et de la liberté d'expression en particulier, le texte évoque à plusieurs reprises les situations dans lesquelles l'hébergeur serait informé de la présence de contenus illicites. Tel est en particulier le statut incertain à cet égard de la notion de modération dont on comprend qu'elle est exercée spontanément par l'hébergeur.

S'il n'y a pas d'obligation de surveillance générale, l'hébergeur exerce bien une forme de surveillance sur les contenus. Dès lors que cette surveillance peut résulter de contrôles effectués à l'aide de « moyens automatisés », c'est-à-dire d'algorithmes, se pose alors la question des critères selon lesquels les hébergeurs exercent ce contrôle aléatoire.

L'absence d'obligation de surveillance générale joue ainsi uniquement au profit des hébergeurs en les libérant de toute responsabilité s'agissant de la présence de contenus illicites sur leurs plateformes. Ainsi, l'article 6 du projet de règlement précise expressément que ces activités « d'enquêtes volontaires » ne sauraient avoir pour effet de remettre en cause le principe d'irresponsabilité des hébergeurs. En revanche, elle ne dit rien des conditions dans lesquelles ces derniers assurent une forme de suivi aléatoire des contenus.

C'est la raison pour laquelle il convient là aussi de faire évoluer le dispositif. Nos démocraties imposent un régime de responsabilité extrêmement contraignant aux éditeurs de presse par exemple, alors même que leur audience est sans commune mesure avec celles des grandes plateformes. Ces contraintes n'ont jamais été perçues comme de nature à entraver la liberté d'expression et ont permis au débat démocratique de se tenir dans de bonnes conditions. Aussi, il semble paradoxal d'affirmer que de nouvelles contraintes opposables désormais aux plateformes, sans atteindre l'intensité de celles s'appliquant aux éditeurs de presse, soient par elles-mêmes de nature à porter atteinte à la liberté d'expression

Le principe de l'absence d'obligation générale de surveillance doit être maintenu. Mais ce sont les conséquences éventuelles que l'hébergeur en tire, s'agissant en particulier de décisions de retrait de contenus ou d'accès, qui doivent évoluer. Or, ce point mérite une attention en tant que tel (voir infra).

De plus, comme on l'a rappelé précédemment, cette « absence d'obligation » n'empêche pas pour autant les hébergeurs d'exercer une certaine forme de surveillance sur les contenus.

Plusieurs propositions additionnelles pourraient ainsi être faites à ce titre.

- Une obligation de surveillance de la part des hébergeurs vis-à-vis des bénéficiaires de service ayant déjà été sanctionnés en raison de la diffusion de contenus illicites ; vis-à-vis de ces personnes, les pouvoirs de retrait de contenus et d'accès des hébergeurs en cas de « récidive » pourraient être renforcés ;
- Une obligation de surveillance pour les bénéficiaires au-delà d'une certaine audience ; il paraît en effet ici légitime de soumettre à une surveillance particulière les personnes dont le nombre d'abonnés est singulièrement important et pour lesquels les

conséquences d'une éventuelle infraction pourraient être particulièrement lourdes ;

- Les plateformes réalisant des opérations de surveillance sur les contenus qu'elles hébergent devraient également rendre compte périodiquement de cette activité auprès des coordinateurs nationaux ; cette obligation permettrait de mesurer l'intensité et la nature des activités effectuées à ce titre.

La question des moyens mis au service de la proscription effective des contenus illicites est légitimement soulevée. Mais, dès lors que l'essentiel de la charge en revient aux plateformes elles-mêmes, par le biais de modération algorithmique ou humaine, la tâche des autorités publiques est de deux natures : le contrôle que les règles des plateformes ne prohibent que les contenus illicites et l'audit de leurs moyens humains ou automatiques de modération, d'une part ; le contrôle juridictionnel des décisions qu'elles prennent, d'autre part.

3.3 LA QUESTION DES RECOURS CONTRE LES RETRAITS DE CONTENUS ET D'ACCÈS

Cette question était la grande absente de la directive du 8 juin 2000. Rien n'était dit sur les conditions dans lesquelles les TGPFL pouvaient retirer de leur propre initiative des contenus qu'ils considèrent comme illicites ou suspendre, voire supprimer, les services qu'ils offrent à certains bénéficiaires.

Or, cette question est cruciale en termes de respect des libertés fondamentales et en particulier de liberté d'expression. On voit également comment une politique de retrait de contenus ou d'accès dans des périodes critiques, telles que les campagnes électorales, pourrait avoir un impact éventuel sur le sens du scrutin et donc sur le fonctionnement global de la démocratie.

L'article 17 met bien en place un système de réclamation, ouvert également aux personnes qui verraient suspendue ou résiliée la fourniture de services. L'article 17.3 indique que ces réclamations doivent être traitées *« en temps opportun de manière diligente et objective ».*

On conviendra que le niveau d'exigence est à ce titre minimal.

Rien ne garantit dans ce texte que l'accès puisse être rétabli suffisamment rapidement pour éviter que cette situation n'ait des effets trop perturbants sur le libre déroulement des débats.

Cela revient à dire que la responsabilité reposera sur un juge national qui ne disposera pas nécessairement des moyens d'intervenir de manière efficace, notamment en face d'une sanction dont la portée dépassera le plus souvent le seul périmètre du territoire national.

De même, les motifs pouvant justifier un retrait de contenu ou d'accès restent flous. Si la notion de contenu illicite est définie par le projet de règlement (cf supra) et vise toute non-conformité au droit national ou européen, le même projet prévoit également que les décisions de retrait peuvent se fonder sur « l'incompatibilité des informations avec les conditions générales du fournisseur » (article 15 du projet de règlement). A ce titre, il convient en particulier de signaler que ces conditions générales font fréquemment référence à des droits étrangers à celui de l'UE et renvoient également à la compétence de juridictions non européennes pour traiter de certains des litiges pouvant apparaître à ce titre.

Ainsi, le code de conduite de mai 2016 indique que les opérateurs examineront les signalements visant au retrait de contenus en ligne « à l'aune de leurs règles et lignes directrices internes, et, si nécessaire, des lois nationales transposant la décision-cadre 2008/913/JAI »[4]. De même, ils doivent informer les utilisateurs des « types de contenus qui ne sont pas autorisés en vertu de leurs règles et lignes directrices internes ».

L'emploi de moyens automatisés est une source de préoccupation en tant que telle, dès lors qu'ils peuvent apparaître *« incapables de faire la différence de manière fiable entre contenu illicite et contenu qui est licite dans un contexte donné »* Résolution du Parlement Européen du 20 octobre 2020.

Dans ce contexte, les propositions suivantes peuvent être avancées.

- Au nom du respect de la liberté d'expression, un retrait de contenu ou d'accès ne doit être justifié que par son caractère illicite, c'est-à-dire méconnaissant une norme européenne ou nationale. Le Parlement européen dans sa résolution du 20 octobre 2020 réclame également une telle modification. On peut d'ailleurs s'interroger sur la constitutionnalité d'un retrait pour un autre motif au regard de la jurisprudence du Conseil constitutionnel qui considère que l'accès libre à internet est aujourd'hui une des modalités du principe constitutionnel de liberté d'expression. S'agissant de la protection des droits d'exploitation des hébergeurs, il serait étonnant que les dispositions civiles et commerciales applicables en ce domaine ne protègent pas sur ce point précis efficacement leurs droits également. Dès lors, « l'incompatibilité avec les conditions générales du fournisseur » ne devrait plus être à l'avenir un motif de retrait de contenu ou d'accès.

- On peut également ici s'interroger sur le point de savoir si certains « éditeurs de contenus » ne devraient pas bénéficier d'une protection renforcée vis-à-vis du risque de retrait de contenu et/ou d'accès. En effet, de telles mesures peuvent avoir un impact majeur sur le déroulement du débat public ou le fonctionnement de la démocratie. Ainsi, on pourrait imaginer une procédure particulière vis-à-vis des bénéficiaires de service suivants : partis politiques, associations bénéficiant d'une reconnaissance particulière de la part de la puissance publique, médias, par exemple. Pour ces derniers, on pourrait imaginer que l'hébergeur n'aurait pas le droit de procéder unilatéralement à une décision de retrait et que celle-ci devrait impérativement être précédée d'une mise en demeure préalable permettant à la personne concernée de faire valoir ses arguments. De même, pour cette catégorie particulière de bénéficiaires, des voies de recours adaptées, notamment juridictionnelles, devraient être aménagées pour leur permettre de contester rapidement et efficacement les décisions de retrait dont ils seraient l'objet.

- Enfin doit également être traitée la question des mesures par lesquelles un hébergeur, sans procéder au retrait même d'un contenu procède à son « invisibilisation », c'est-à-dire tend à le faire disparaître par des dispositifs de filtrage perfectionnés. Ces procédés ne doivent pas être négligés car ils aboutissent à une forme de quais-retrait de contenu, sans aucune garantie pour la personne qui l'a émis. Cette situation potentiellement grave, outre qu'elle renvoie à la question d'une activité de véritable éditeur de contenu joué alors par la plateforme, doit être prise en compte et susciter

[4] *Il s'agit de la décision cadre du Conseil sur la lutte contre certaines formes et manifestations de racisme et de xénophobie au moyen du droit pénal. Son article 1er prescrit aux Etat membres d'édicter des sanctions pénales contre toute incitation à la violence ou à la haine quel que soit le support sur lequel ce type de messages est diffusé*

un traitement particulier, soit en imposant à l'hébergeur de notifier à l'auteur du contenu la « décision » ainsi prise, soit en l'interdisant purement et simplement.

3.4 LA QUESTION DE L'ANONYMAT

C'est la grande absente de ce texte qui ne dit rien de cette question.

Or, celle-ci est fondamentale. Comme le rappelle la CNCDH dans son rapport précité de 2015 *« la possibilité de l'anonymat et l'utilisation du pseudonyme qui entraînent un fort sentiment d'impunité »* sont une des premières causes du développement de la haine sur internet.

Cette question est majeure car elle pose la question de **l'effectivité de la sanction** dès lors que l'auteur des propos incriminés échappera dans les faits aux poursuites.

Il ne s'agit pas dans notre esprit de remettre en cause l'anonymat, mais de rendre incontournable la transmission des données d'identification dans le cas où elles sont nécessaires pour le bon fonctionnement de la justice.

Le texte devrait **imposer une obligation aux bénéficiaires de service de faire la preuve de leur identité pour pouvoir accéder à ceux-ci**. Cela constituerait également un moyen efficace d'éviter la présence de mineurs sur des services auxquels ils ne devraient pas normalement avoir accès.

A cet égard, l'article 8 du projet de règlement sur les injonctions susceptibles d'être adressées aux hébergeurs par les autorités nationales apparaît largement insuffisant pour lutter contre l'impossibilité de transmettre aux autorités juridictionnelles les données d'identification. Cette question doit donc respecter une distinction majeure.

La transmission des données ne doit concerner que les hébergeurs. En effet, pour que les mesures de retrait soient efficaces, il faut qu'elles puissent s'appliquer effectivement aux personnes qui sont les auteurs des contenus concernés. De même, si l'infraction nécessite que la justice soit saisie, il est normal que cette dernière puisse effectivement poursuivre les personnes responsables, après que leur identité aura été communiquée par l'hébergeur.

En revanche, il ne saurait être question d'une quelconque levée d'anonymat vis-à-vis des tiers. Il peut d'abord s'agir des autres bénéficiaires du même service, l'anonymat pouvant alors protéger l'auteur des contenus de certaines formes de rétorsion aux propos mis en ligne. L'anonymat est alors une forme de protection de la liberté d'expression.

Il en va particulièrement des tiers dont la connaissance de l'auteur des contenus pourrait nuire gravement aux intéressés. Tel est par exemple le cas des lanceurs d'alerte qui doivent pouvoir être protégés par la règle de l'anonymat, sous peine de les exposer fortement à des risques élevés alors qu'ils jouent leur rôle.

Il est à noter que la loi du 22 décembre 2018 relative à la lutte contre la manipulation de l'information impose déjà aux opérateurs de PFL des obligations d'information des utilisateurs de leurs services sur les personnes physiques ou morales qui leur versent des rémunérations en contrepartie de la promotion de contenus d'information se rattachant à un débat d'intérêt général.

Cette mesure ne nous paraît de nature à menacer la liberté individuelle, dans nos démocraties. Les dispositifs de protection des droits et libertés sont suffisamment efficaces et éprouvés pour pouvoir mettre à l'abris les citoyens d'une utilisation de cette faculté qui serait ici susceptible de mettre en péril leur situation ou leurs droits.

CONCLUSION

La proposition de la Commission du 15 décembre 2020 constitue un progrès indéniable au regard du caractère lacunaire de la règlementation issue de la directive du 8 juin 2000. Cette directive, principalement élaborée aux fins de permettre le développement des échanges sur internet dans le cadre de l'achèvement du marché intérieur, est aujourd'hui dépassée : elle ne prend pas en compte les formidables développements technologiques et d'usage intervenus depuis lors.

Des avancées importantes figurent dans la proposition de la Commission. Elles méritent d'être soutenues. Son parcours d'adoption risque d'être semé d'embûches devant le Conseil et le Parlement européen.

Toutefois, on peut s'interroger sur son manque d'ambition sur certains points fondamentaux. En maintenant le principe d'irresponsabilité des hébergeurs et d'absence d'obligation de surveillance généralisée, elle ne modifie pas les fondements d'un système juridique qui, jusqu'à présent, a surtout montré ses insuffisances.

De même, la question majeure des retraits de contenus et d'accès décidés unilatéralement par les hébergeurs et qui peuvent gravement perturber le fonctionnement de nos démocraties reste traitée de manière trop légère dans cette proposition.

Enfin, la question de « l'irresponsabilité de fait » des auteurs de contenus illicites, par l'absence de données d'identification, n'est pas abordée, alors même qu'elle assure une forme d'impunité intolérable.

Soutenir la proposition de la Commission ne suffira pas à résoudre les formidables défis qu'internet pose à nos démocraties. L'amender en profondeur est une absolue nécessité. Ce pourrait être l'un des objectifs de la présidence française de l'Union Européenne qui commence en janvier 2022.

DIGITAL NEW DEAL
LE THINK-TANK DE LA NOUVELLE DONNE

Le think tank Digital New Deal a pour vocation d'éclairer de la manière la plus complète possible les évolutions à l'œuvre au sein du phénomène de «digitalisation», dans l'acception la plus large du mot, et d'élaborer des pistes d'actions concrètes à destination des entreprises et des décideurs publics français et européens. Portés par l'expertise de leurs rédacteurs et leur insertion dans le débat public, les travaux du think tank pourront participer à l'élaboration d'une pensée française et européenne de la régulation digitale au service de la mise en place d'un cadre équilibré et durable.

LE CONSEIL D'ADMINISTRATION

Les membres du Conseil d'administration de Digital New Deal sont tous membres fondateurs. Ils sont issus d'horizons divers tout en étant en prise directe avec la transformation digitale des entreprises et des organisations. Forts de leur intérêt commun pour les questions numériques, ils ont décidé d'approfondir leurs débats en formalisant un cadre de production et de publication au sein duquel la complémentarité de leurs expériences pourra être mise au service du débat public et politique. Ils s'impliquent personnellement dans la vie de Digital New Deal.

Arno Pons, délégué général, pilote avec Olivier Sichel, président fondateur, les orientations stratégiques de la fondation, et supervise un chargé de mission qui assure la coordination, au quotidien, de l'ensemble des activités du think tank.

SÉBASTIEN BAZIN
PDG AccorHotels

NICOLAS DUFOURCQ
DG de Bpifrance

AXELLE LEMAIRE
Ex-Secrétaire d'Etat du Numérique et de l'Innovation

ALAIN MINC
Président AM Conseil

DENIS OLIVENNES
DG Libération

YVES POILANE
DG Ionis Education Group

ARNO PONS
Délégué général du think tank Digital New Deal

JUDITH ROCHFELD
Professeur agrégée de Droit, Panthéon Sorbonne

OLIVIER SICHEL
President Digital New Deal
DGA Caisse des Dépôts

ROBERT ZARADER
PDG Equancy

contact@thedigitalnewdeal.org

www.thedigitalnewdeal.org

NOS PUBLICATIONS

Cloud de confiance : un enjeu d'autonomie stratégique pour l'Europe
Laurence Houdeville et Arno Pons - *mai 2021*

Livres blancs : Partage des données & tourisme
Fabernovel et Digital New Deal - *avril 2021*

Partage de données personnelles : changer la donne par la gouvernance
Personal data sharing: governance as a game changer
Matthias de Bièvre et Olivier Dion - *septembre 2020*

Paiement mobile sans contact – libérer les smartphones et leurs utilisateurs
Contactless mobile payment : liberating smartphones and their users
Various - *juin 2020*

Réflexions dans la perspective du Digital Services Act européen
Reflections in the perspective of the European Digital Services Act
Liza Bellulo - *mars 2020*

Préserver notre souveraineté éducative : soutenir l'EdTech française
Marie-Christine Levet - *novembre 2019*

Briser le monopole des Big Tech : réguler pour libérer la multitude
Big Tech Regulation: Empowering the Many by Regulating A Few
Sébastien Soriano - *septembre 2019*

Sortir du syndrome de Stockholm numérique
Jean-Romain Lhomme - *octobre 2018*

Le Service Public Citoyen
Paul Duan - *juin 2018*

L'âge du web décentralisé
Clément Jeanneau - *avril 2018*

Et si le CAC 40 ubérisait…sa R&D
Paul-François Fournier - *novembre 2017*

Fiscalité réelle pour un monde virtuel
Vincent Renoux - *septembre 2017*

Réguler le « numérique »
Joëlle Toledano - *mai 2017*

Appel aux candidats à l'élection présidentielle pour un #PacteNumérique
janvier 2017

La santé face au tsunami des NBIC et aux plateformistes
Laurent Alexandre - *juin 2016*

Quelle politique en matière de données personnelles ?
Judith Rochfeld - *septembre 2015*

Etat des lieux du numérique en Europe
Olivier Sichel - *juillet 2015*

THINK-TANK
DIGITAL
NEW DEAL

juin 2021

www.thedigitalnewdeal.org